Adaptaciones del Protocolo BGP-4 para Reducir la Congestión en Redes IP

Andrés Arturo Delgado Vallejo

Daniel Andrés Sánchez Sánchez

Universidad del Cauca

Facultad de Ingeniería Electrónica y Telecomunicaciones

Departamento de Telecomunicaciones

Grupo de Nuevas Tecnologías en Telecomunicaciones

Popayán, Marzo de 2010

Adaptaciones del Protocolo BGP-4 para Reducir la Congestión en Redes IP

Andrés Arturo Delgado Vallejo

Daniel Andrés Sánchez Sánchez

Monografía para optar al título de
Ingeniero en Electrónica y Telecomunicaciones

Director: Ing. Jenny Cuatindioy Imbachi

Universidad del Cauca

Facultad de Ingeniería Electrónica y Telecomunicaciones

Departamento de Telecomunicaciones

Grupo de Nuevas Tecnologías en Telecomunicaciones

Popayán, Marzo de 2010

Eterna gratitud a los seres que alumbraron mi vida e hicieron realidad este sueño.
A mis hermanos, Iván Darío y José David por su presencia y acompañamiento en mi carrera profesional.

Andrés Arturo Delgado Vallejo

Con un profundo agradecimiento a mis padres, Martha Isabel Sánchez y Felipe Alberto Restrepo, quienes con su guía y gran amor, impulsaron mi carrera. A mi hermana, Manuela, por su gran apoyo, por compartirme su alegría y dulzura.

Daniel Andrés Sánchez Sánchez

AGRADECIMIENTOS

Los autores expresan su agradecimiento:

A la Universidad del Cauca y a la FIET por su formación académica y crecimiento en valores.

A la Ingeniera Jenny Cuatindoy Imbachi gratitud por sus valiosas orientaciones.

Al Ingeniero Francisco Javier Terán y Oscar Josué Calderón por su apoyo incondicional en la búsqueda del conocimiento.

Por último y no menos importante, el más afectuoso agradecimiento a nuestras familias, quienes nos apoyaron incondicionalmente, no solo en este trabajo de grado, si no en toda la realización de la carrera ingenieril.

El haber llegado hasta este punto en nuestras carreras académicas y personales ha sido gracias a Uds.

Los Autores
Popayán, Marzo de 2010

TABLA DE CONTENIDO

INTRODUCCIÓN 1
CAPITULO I: GENERALIDADES DE ENRUTAMIENTO, PROTOCOLO BGP, INGENIERÍA DE TRÁFICO Y CONGESTIÓN EN UNA RED IP 3
1.1 ENRUTAMIENTO 4
1.1.1 Protocolos de Vector Distancia 6
1.1.2 Protocolos de Estado de Enlace 8
1.2 EL PROTOCOLO BGP 9
1.2.1 Mensajes BGP 11
1.2.2 Atributos BGP 11
1.2.3 Proceso de Enrutamiento con el protocolo BGP-4 14
1.3 INGENIERÍA DE TRÁFICO 15
1.4 CONGESTIÓN 17
1.4.1 Pérdida de Paquetes como Indicador de Congestión 18
CAPITULO II: ADAPTACIONES DEL PROTOCOLO BGP BAJO CONSIDERACIONES DE TE Y QOS 19
2.1 MÉTRICAS DE ENRUTAMIENTO 19
2.2 INTRODUCCIÓN A LA OPTIMIZACIÓN DEL PROTOCOLO BGP 20
2.3 MECANISMOS ACTUALES QUE IMPLEMENTAN CAPACIDADES DE TE CON EL PROTOCOLO BGP-4 21
2.3.1 Communities 22
2.3.2 Otros Mecanismos 23
2.4 CONSIDERACIONES PARA MEJORAR LA TOMA DE DECISIONES DE ENRUTAMIENTO EN BGP-4 TENIENDO EN CUENTA TE 26
2.5 SOLUCIÓN PROPUESTA PARA LA REDUCCIÓN DE LA CONGESTIÓN EN REDES IP MEDIANTE ADAPTACIÓN DEL PROTOCOLO BGP-4 26
2.5.1 Congestión de Ruta 29
2.5.2 Pérdida de Paquetes de Información 31
2.5.3 Pérdida de Bytes de Información 31
2.5.4 Costo de la Ruta 31
2.5.5 El Atributo LOCAL_PREFERENCE 32
CAPITULO III: SIMULACIONES, PRUEBAS Y RESULTADOS 33
3.1 ESCENARIOS DE SIMULACIÓN 34
3.1.1 Escenario de Simulación No1 34
3.1.2 Escenario de Simulación No2 35

3.1.3 Escenario de Simulación No3 36
3.1.4 Escenario de Simulación No4 37
3.2 SIMULACIONES 38
3.2.1 Escenario1 39
3.2.1.1 Escenario1: BGP-4 39
3.2.1.2 Escenario1: BGP-C2 en t1 40
3.2.1.2.1 Gráfica de Paquetes y Bytes Perdidos vs Tasa de Pérdidas. 41
3.2.1.3 Escenario1: BGP-C2 en t2 43
3.2.1.3.1 Gráficas de Paquetes y Bytes Perdidos vs Tasa de Pérdidas. 43
3.2.1.4 Escenario1: BGP-C2 en t3 45
3.2.1.4.1 Gráfica de Paquetes y Bytes Perdidos vs Tasa de Pérdida. 46
3.2.2 Escenario2 48
3.2.2.1 Escenario2: BGP-4 48
3.2.2.2 Escenario2: BGP-C2 en t1 49
3.2.2.2.1 Gráficas de Paquetes y Bytes Perdidos vs Tasa de Pérdida. BGP-C2 50
3.2.2.3 Escenario2: BGP-C2 en t2 52
3.2.2.3.1 Gráfica de Paquetes y Bytes Perdidos vs Tasa de Pérdida. BGP-C2 52
3.2.3 Escenario 3 54
3.2.3.1 Escenario3: BGP-4 54
3.2.3.2 Escenario3: BGP-C2 en t1 56
3.2.3.2.1 Gráfica de Paquetes Bytes Perdidos vs Índice de Pérdida. 56
3.2.3.3 Escenario3: BGP-C2 en t2 57
3.2.3.3.1 Gráfica de Paquetes y Bytes Perdidos vs Tasa de Pérdida. 58
3.2.4 Escenario4 60
3.2.4.1 Escenario4: BGP-4 60
3.2.4.2 Escenario4: BGP-C2 en t1 61
3.2.4.2.1 Gráfica de Paquetes y Bytes Perdidos vs Tasa de Pérdida. 62
3.2.4.3 Escenario4: BGP-C2 en t2 64
3.2.4.3.1 Gráfica de Paquetes y Bytes Perdidos vs Tasa de Pérdida. 64
CAPITULO IV: CONCLUSIONES Y RECOMENDACIONES 67
BIBLIOGRAFIA 71

Índice De Figuras

Figura 1 Proceso de Enrutamiento Básico 5
Figura 2 Proceso de Enrutamiento Básico de BGP 21
Figura 3 Mecanismo que hace uso del Atributo Communities 23
Figura 4 Proceso de Enrutamiento de BGP Modificado 29
Figura 5 Escenario de Simulación1 35
Figura 6 Escenario de Simulación 2 36
Figura 7 Escenario de Simulación 3 37
Figura 8 Escenario de Simulación 4 37
Figura 9 Tabla de Enrutamiento de R1 presente en el AS1. BGP-4. Escenario1. 39
Figura 10 Paquetes recibidos en el Servidor HTTP sin Congestión. BGP-4 Escenario 1 40
Figura 11 Paquetes recibidos en el Servidor HTTP con Congestión. BGP-4 Escenario 1 40
Figura 12 Tabla de Enrutamiento R1 presente en el AS1. Protocolo BGP-C2 en t1. Escenario 1. 41
Figura 13 Paquetes Perdidos vs. Tasa de Pérdida. BGP-C2 42
Figura 14 Bytes Perdidos vs. Tasa de Pérdidas. BGP-C2 42
Figura 15 Tabla de Enrutamiento R1 presente en el AS1 Protocolo BGP-C2 en t2 Escenario 1. 43
Figura 16 Paquetes Perdidos vs. Tasa de Pérdida. BGP-C2 44
Figura 17 Bytes Perdidos vs. Tasa de Pérdida.BGP-C2 45
Figura 18 Tabla de Enrutamiento R1 presente en el AS1. Protocolo BGP-C2 en t3 Escenario 1. 46
Figura 19 Paquetes Perdidos vs. Tasa de Pérdida.BGP-C2 47
Figura 20 Bytes Perdidos vs. Tasa de Pérdida.BGP-C2 48
Figura 21 Tabla de Enrutamiento R1 presente en el AS1. Protocolo BGP-4 Escenario 2 48
Figura 22 Paquetes recibidos en el Servidor HTTP sin Congestión. BGP-4 Escenario 2. 49
Figura 23 Paquetes recibidos en el Servidor HTTP con Congestión. BGP-4. Escenario 2 49
Figura 24 Tabla de Enrutamiento R1 presente en AS1. Protocolo BGP-C2 en t1. Escenario 2. 50
Figura 25 Paquetes Perdidos vs. Tasa de Pérdida. BGP-C2 51
Figura 26 Bytes Perdidos vs. Tasa de Pérdida. BGP-C2 51
Figura 27 Tabla de Enrutamiento R1 presente en el AS1. Protocolo BGP-C2 en t2 Escenario 2. 52
Figura 28 Paquetes Perdidos vs. Tasa de Pérdida. BGP-C2 53
Figura 29 Bytes Perdidos vs. Tasa de Pérdida. BGP-C2 54
Figura 30 Tabla de Enrutamiento R1 presente en el AS1. Protocolo BGP-4 Escenario 3. 54
Figura 31 Paquetes recibidos en el Servidor HTTP sin Congestión. BGP-4 Escenario 3. 55
Figura 32 Paquetes recibidos en el Servidor HTTP con Congestión. BGP-4 Escenario 3 55

Figura 33 Tabla de Enrutamiento de R2 presente en el AS1. BGP-C2 en t1 Escenario 3. 56
Figura 34 Paquetes Perdidos vs. Tasa de Pérdida. BGP-C2 57
Figura 35 Bytes Perdidos vs. Tasa de Pérdida. BGP-C2 57
Figura 36 Tabla de Enrutamiento de R2 presente en el AS1. BGP-C2 en t2 Escenario 3. 58
Figura 37 Paquetes Perdidos vs. Tasa de Pérdida. BGP-C2 59
Figura 38 Bytes Perdidos vs. Tasa de Pérdida. BGP-C2 59
Figura 39 Tabla de Enrutamiento R1 presente en el AS1 Protocolo BGP-4 Escenario 4. 60
Figura 40 Paquetes recibidos en el Servidor HTTP sin Congestión. BGP-4 Escenario 4. 61
Figura 41 Paquetes recibidos en el Servidor HTTP con Congestión. BGP-4 Escenario 4. 61
Figura 42 Tabla de Enrutamiento R1 y R2 presentes en el AS1. BGP-C2 en t1 Escenario 4... 62
Figura 43 Paquetes Perdidos vs. Tasa de Pérdida. BGP-C2 63
Figura 44 Bytes Perdidos vs. Tasa de Pérdida. BGP-C2 63
Figura 45 Tabla de Enrutamiento R1 y R2 presentes en el AS1. BGP-C2 en t2 Escenario 4.... 64
Figura 46 Paquetes Perdidos vs Tasa de Pérdida BGP-C2 65
Figura 47 Bytes Perdidos vs. Tasa de Perdida. BGP-C2 65

ÍNDICE DE TABLAS

Tabla 1 Métricas de Enrutamiento más Utilizadas..... 20
Tabla 2 Otros Mecanismos para Optimización..... 24
Tabla 3 Condiciones de Red..... 33
Tabla 4 Congestión presente en cada Ruta. Escenario 1 BGP-C2 en t1..... 41
Tabla 5 Paquetes Perdidos y Tasa de Pérdida en la Ruta 1. Escenario 1 BGP-C2..... 41
Tabla 6 Bytes Perdidos y Tasa de Pérdida en la Ruta1. Escenario 1 BGP-C2..... 42
Tabla 7 Congestión presente en cada Ruta. Escenario1 BGP-C2 en t2..... 43
Tabla 8 Paquetes Perdidos y Tasa de Pérdida en la Ruta2. Escenario1 BGP-C2 44
Tabla 9 Bytes Perdidos y Tasa de Pérdida en la Ruta2. Escenario1 BGP-C2..... 44
Tabla 10 Congestión presente en cada Ruta. Escenario 1 BGP-C2 en t3..... 46
Tabla 11 Paquetes Perdidos y Tasa de Pérdida en la Ruta3. Escenario 1 BGP-C2..... 47
Tabla 12 Bytes Perdidos y Tasa de Pérdida en la Ruta3. Escenario1 BGP-C2..... 47
Tabla 13 Congestión presente en cada Ruta. Escenario2 BGP-C2 en t1..... 50
Tabla 14 Paquetes Perdidos vs Tasa de Pérdida en la Ruta1. Escenario2 BGP-C2..... 50
Tabla 15 Bytes Perdidos vs Tasa de Pérdida en la Ruta1. Escenario2 BGP-C2..... 51
Tabla 16 Congestión presente en cada Ruta. Escenario 2 BGP-C2 en t2..... 52
Tabla 17 Paquetes Perdidos vs Tasa de Pérdida en la Ruta2. Escenario2 BGP-C2..... 53
Tabla 18 Bytes Perdidos vs Tasa de Pérdida en la Ruta2. Escenario2 BGP-C2..... 53
Tabla 19 Congestión presente en cada Ruta. Escenario 3 BGP-C2 en t1..... 56

Tabla 20 Paquetes Perdidos vs Tasa de Pérdida en la Ruta1. Escenario 3 BGPC-2..... 56
Tabla 21 Bytes Perdidos vs Tasa de Pérdida en la Ruta1. Escenario 3 BGP-C2..... 57
Tabla 22 Congestión presente en cada Ruta. Escenario 3. BGP-C2 en t2..... 58
Tabla 23 Paquetes Perdidos vs Tasa de Pérdida en la Ruta2. Escenario 3 BGP-C2..... 58
Tabla 24 Bytes Perdidos vs Tasa de Pérdida en la Ruta2. Escenario 3 BGP-C2..... 59
Tabla 25 Congestión presente en cada Ruta. Escenario 4. BGP-C2 en t1..... 62
Tabla 26 Paquetes Perdidos vs Tasa de Pérdida en la Ruta1. Escenario 4 BGP-C2..... 62
Tabla 27 Bytes Perdidos vs Tasa de Pérdida en la Ruta1. Escenario 4 BGP-C2..... 63
Tabla 28 Congestión presente en cada Ruta. Escenario 4. BGP-C2 en t2..... 64
Tabla 29 Paquetes Perdidos vs Tasa de Pérdida en la Ruta2. Escenario 4 BGP-C2..... 64
Tabla 30 Bytes Perdidos vs Tasa de Pérdida en la Ruta2. Escenario 4 BGP-C2..... 65

INTRODUCCIÓN

Desde la década de los 80's, Internet se ha convertido en una amplia red de información que está siendo operada por una gran cantidad de entidades administrativas conocidas como dominios. Una de las mayores preocupaciones en la industria de las redes de telecomunicaciones en los últimos años, ha sido la optimización de los procesos de enrutamiento, debido al vertiginoso aumento en la demanda de acceso a Internet y la utilización de aplicaciones en tiempo real, por tal motivo se requiere de sistemas, procesos y políticas de enrutamiento óptimos para la eficiente administración de los recursos de red. Bajo las condiciones actuales de las redes, la decisión de enrutamiento basada en el camino más corto, no es suficiente para satisfacer necesidades generales y particulares de los dominios dentro del proceso de enrutamiento; conllevando a que los ISP configuren sus enrutadores de diferentes maneras para satisfacer dichas necesidades [1].

Dentro de los estudios realizados con el propósito de contribuir a la optimización de los procesos de enrutamiento, se observa que el manejo eficiente de los recursos de red, se alcanza mediante la inclusión de capacidades de Ingeniería de Tráfico (TE: Traffic Engineering) en los protocolos de enrutamiento, teniendo como premisa alcanzar niveles adecuados de Calidad del Servicio (QoS: Quality Of Service) [2].

La TE es una rama de la ingeniería que busca un mayor aprovechamiento de los recursos en una red, enfocando sus esfuerzos a garantizar un alto rendimiento en aplicaciones de tiempo real que requieran de recursos como ancho de banda, capacidad de buffer, velocidad de procesamiento en los equipos centrales, entre otros recursos, en pro de lograr un alto desempeño [2].

El Protocolo de Pasarela de Frontera (BGP: Border Gateway Protocol), es actualmente uno de los protocolos de enrutamiento inter-dominio más utilizados, aunque es de rápida convergencia y efectividad, no considera de forma autónoma aspectos importantes dentro de las redes tales como el retardo en los enlaces, el ancho de banda, la congestión, entre otros. Sin embargo, se han realizado diversos estudios relacionados con la temática, sin encontrarse soluciones que permitan superar estas deficiencias. Frecuentemente, los dispositivos de enrutamiento al basarse en el protocolo BGP estándar, envían la información por rutas que no son las mejores existiendo caminos alternos que cuentan con recursos de red necesarios y/o suficientes para evitar la pérdida de información entre un origen y un destino; por lo anterior, la capacidad que tienen los enrutadores de dirigir la información por la ruta que cumpla cualquier tipo de requerimientos en una red, dependerá directamente de la optimización del protocolo BGP que implementen [3] - [4].

Según lo expuesto anteriormente, el objetivo general de este proyecto, consiste en proponer una adaptación al protocolo BGP-4, para mejorar la toma de decisiones de enrutamiento, considerando la congestión como parámetro de red.

Para sustentar el cumplimiento del objetivo en mención, se establecen cuatro capítulos que abordan los temas de interés para el desarrollo del proyecto; dichas secciones expresan lo siguiente:

Capítulo I. Generalidades de Enrutamiento, Protocolo BGP, Ingeniería de Tráfico y Congestión en una Red IP. El primer capítulo del proyecto, presenta brevemente la historia de Internet y su influencia en la evolución de los protocolos de enrutamiento para el manejo de la información. Asimismo, sienta una base conceptual clara del enrutamiento BGP como función de la selección de una ruta, explicando detalladamente su funcionamiento y sus criterios de selección. Por otro lado, esta sección del documento, aborda temas relacionados con Ingeniería de Tráfico, rama de la ingeniería que estudia el aprovechamiento de los recursos de la red y Congestión como parámetro que afecta directamente el desempeño de la red.

Capítulo II. Optimización del Protocolo BGP-4 bajo Consideraciones de TE y Q_oS: este capítulo, contiene la descripción de diferentes mecanismos que implementan capacidades de TE, utilizando los atributos del protocolo BGP-4, métricas de enrutamiento y políticas propuestas por los administradores de red, en la búsqueda de un mejor desempeño del protocolo BGP-4 con su respectiva modificación. Basándose en el análisis anterior, se propone una solución que permita reducir la congestión en una red IP, mediante la adaptación del protocolo de enrutamiento BGP-4 por medio de sus atributos y métricas, con el fin de ser evaluada posteriormente.

Capítulo III. Simulación, Pruebas y Resultados. De acuerdo a la solución propuesta en el capitulo anterior, este aparte indica los escenarios de red utilizados para simular la adaptación propuesta al protocolo. Cabe resaltar que estos escenarios fueron tomados de la tesis de grado *"Estudio de Viabilidad para la Optimización de Enrutamiento IP con el Protocolo BGP"*, considerando que estos son transparentes al objetivo de investigación del proyecto, debido a que no inciden en los resultados esperados. Por otro lado, se muestran los resultados de la simulación para diferentes pruebas realizadas, así como también sus análisis.

Capítulo IV. Conclusiones, Recomendaciones y Trabajos Futuros. En este capítulo final, se establece una serie de conclusiones respecto a la propuesta planteada en este proyecto, respecto a la simulación y a la herramienta utilizada, como también una descripción de los posibles trabajos futuros referentes al tema.

CAPITULO I: GENERALIDADES DE ENRUTAMIENTO, PROTOCOLO BGP, INGENIERÍA DE TRÁFICO Y CONGESTIÓN EN UNA RED IP

En la década de 1950, durante la guerra fría, los Estados Unidos buscaban formas de protegerse de los ataques soviéticos. Una de las estrategias para lograrlo fue la creación de la Agencia de Proyectos de Investigación Avanzada (ARPA: Advanced Research Projects Agency), ahora conocida como Agencia de Proyectos de Investigación Avanzada de Defensa (DARPA: Defense Advanced Research Projectss Agency), organización encargada de crear tecnología capaz de brindar seguridad a su país. A principios de 1962 surgen las primeras ideas para interconectar computadores e intercambiar información de forma electrónica [2].

En 1968, ARPANET fue la primera red de computadores, años más tarde después de un crecimiento excepcional, se consolida en lo que hoy en día se conoce como Internet. Dicha red era considerada como la unión de pequeñas redes privadas conectadas entre sí para el intercambio de información. Desde mediados de los 80`s se ha vislumbrado un alto crecimiento tecnológico en el área de servicios de telecomunicaciones debido a la gran acogida de Internet por parte de los usuarios finales, quienes exigían más y mejores servicios de entretenimiento e información. Esto conllevó al incremento del tráfico de paquetes en las redes IP, por lo cual se hizo necesario contar con protocolos de enrutamiento que permitieran direccionar eficientemente la información, garantizando que los paquetes que se trasportaban por la red, lleguen de manera confiable y sin retardos a su destino [2].

Para interconectar diferentes redes, optimizar sus recursos y lograr que la información que circula por ellas se entregue de manera confiable, se crearon protocolos y algoritmos de enrutamiento, cuya función consistía en enviar los datos, seleccionando una ruta que presentara el menor número de saltos entre su origen y su destino como condición de envío. Esta condición fue complementada con exigencias externas, comúnmente políticas administrativas o económicas.

Entre los protocolos de enrutamiento más difundidos se encuentran RIP, OSPF, iGRP, eiGRP que operan a nivel intra-dominio; y a nivel inter-dominio se encuentran EGP y BGP. Los anteriores protocolos en su mayoría direccionan la información tomando como premisa la ruta más corta. Inicialmente, se implementó el Protocolo de Pasarela Exterior (EGP: Exterior Gateway Protocol) para intercambiar información de acceso entre el backbone y las redes regionales; al presentarse un rápido aumento en el tamaño de las redes y el tráfico de datos, se adoptó el Protocolo de Pasarela de Frontera (BGP: Border Gateway Protocol) para realizar el enrutamiento entre dominios en Internet.

Ahora bien, tanto para los Proveedores de Tecnología como para los Proveedores de Servicios de Internet (ISP: Internet Service Provider), es indispensable ofrecer Calidad de Servicio (QoS: Quality of Service) frente a los requerimientos de las aplicaciones y exigencias actuales de los usuarios, para operar competitivamente en el mercado de las telecomunicaciones.

El presente capitulo es parte fundamental en el desarrollo del proyecto, porque contiene una base teórica donde se abordan temas como principios básicos de enrutamiento, funcionamiento del protocolo BGP y TE, siendo este ultimo una rama de la ingeniería que permite optimizar recursos de red y congestión que representa un problema critico que afecta directamente el desempeño de una red y sus posibles soluciones.

1.1 ENRUTAMIENTO

Internet desde el punto de vista lógico y físico se considera una red conformada por redes más pequeñas conocidas como dominios o Sistemas Autónomos (AS: Autonomous System), son redes o grupos de redes bajo una misma administración que se rigen mediante políticas comunes claramente definidas. Entre algunos ejemplos de AS se encuentran las grandes empresas, universidades y los ISP, entre otros. La interconexión entre los AS se realiza por medio de enlaces físicos ya sean cableados o inalámbricos según la tecnología utilizada [5] - [6].

Los dominios en Internet se distinguen por tener enrutadores de núcleo, cuya función es permitir el intercambio de información a nivel intra-dominio, ya que conocen el estado de los enlaces y de los nodos que conforman dicho dominio; también poseen enrutadores de frontera, que se encargan de procesar el tráfico entrante y saliente del AS al que pertenecen, es decir, el trafico inter-dominio. Todos los AS se identifican en la red con un número conocido como Número de Sistema Autónomo (ASN: Autonomous System Number), éste corresponde a un identificador global y único para cada dominio y es asignado por la Autoridad para la Asignación de Números de Internet (IANA: Internet Assigned Numbers Authority) [6] - [7].

El enrutamiento es uno de los procesos más importantes y complejos en el intercambio de información, ubicándose en el Nivel de Red del Modelo de Referencia de Interconexión de Sistemas Abiertos (OSI: Open Systems Interconnect) o en la Capa de Internet del Modelo Protocolo de Control de Transmisión/Protocolo de Internet (TCP/IP: Transmission Control Protocol/Internet Protocol); dichos niveles tienen como función conectar los dispositivos de enrutamiento utilizando IP. Los enrutadores son dispositivos hardware o software que funcionan como enlaces para interconectar redes de telecomunicaciones, los cuales se identifican, considerando el proceso de direccionamiento, por medio de la dirección IP; actualmente, la más utilizada en Internet es la versión 4 (IPv4) donde la dirección IP consta de 32 bits, que por facilidad de manejo se separan en grupos de 8 bits cada uno, sin embargo se implementó la versión 6 (IPv6), que permite crear una cantidad mucho mayor de direcciones de red. Estos dispositivos de enrutamiento permiten, la circulación de tráfico de información dentro de un mismo AS como también entre diferentes AS que conforman Internet. Por lo anterior se clasifica el tráfico en Intra-dominio e Inter-dominio respectivamente [5].

El proceso de enrutamiento es más complejo de lo que parece, considerando que un enrutador se encuentra conectado a una gran cantidad de redes, las cuales a su vez se conectan a otras redes que son invisibles al dispositivo de enrutamiento. Por lo anterior, para el envío y recepción de información, los enrutadores operan utilizando protocolos de enrutamiento en conjunto con tablas de enrutamiento, según el siguiente modelo [8].

1. Los enrutadores crean y actualizan sus tablas de enrutamiento para intercambiar información con sus vecinos, sobre las posibles rutas para alcanzar el destino.

2. El enrutador recibe una trama de bits de información, la cual proviene de un dispositivo transmisor origen que se encuentra conectado a la misma red del enrutador.

3. La información es transmitida al nivel de Red.

4. El dispositivo de enrutamiento observa la dirección IP del destino contenida en el paquete y la compara con la información que tienen en sus tablas de enrutamiento. Si la

dirección IP destino pertenece a una red conectada a una de las interfaces del enrutador, la información es enviada al destino, después de haber sido adaptada al nivel de transporte.

5. Se ejecuta el proceso de enrutamiento para enviar la información por la "mejor ruta".

6. El enrutador envía la información al destino, considerando la mejor ruta seleccionada por los algoritmos de enrutamiento.

Si el receptor no hace parte de la red donde se encuentra el enrutador origen, el modelo anterior se repite hasta que la dirección IP destino, coincida con la información de la tabla de enrutamiento del dispositivo trasmisor [8].

En la figura 1 se muestra una síntesis del modelo utilizado por los enrutadores para enviar y recibir información, considerando los protocolos en conjunto con las tablas de enrutamiento.

Figura 1 Proceso de Enrutamiento Básico

El enrutamiento debe considerar procesos de enrutamiento tanto estáticos como dinámicos para el trasporte de tráfico en la red. En el primer caso, no se calcula la ruta completa desde el origen hasta el destino, únicamente se tiene en cuenta el dispositivo del próximo salto, el cual a su vez considera la información de su tabla de enrutamiento para enviar la información al siguiente destino, este proceso se repite hasta que los paquetes lleguen al receptor.

El enrutamiento estático posee ventajas frente al dinámico; una de ellas es que el administrador de red, crea y conoce de antemano las tablas de enrutamiento de cada dispositivo, lo que hace posible determinar el número de saltos necesarios para alcanzar a un destino particular, facilitando la configuración de dichos enrutadores. La mayor desventaja es la escalabilidad, y se entiende que por cada dispositivo agregado o eliminado de la red, el administrador deberá actualizar todas las tablas de los dispositivos de enrutamiento pertenecientes a la misma, por tal motivo para redes pequeñas se considera conveniente la implementación del enrutamiento estático [9].

El enrutamiento dinámico como opción para el trasporte de información, posee ventajas frente al estático y es precisamente en la escalabilidad y adaptabilidad a cambios en la topología de la red, ya sea por la agregación de enrutadores o inclusive por la presencia de fallas que puedan originarse por la caída de segmentos de red. Esto se presenta, por que los dispositivos de enrutamiento tienen la capacidad de enviar y recibir información permanente sobre sus rutas disponibles sin necesidad de volver a ser configurados por el administrador de red [9].

Los protocolos de enrutamiento son los encargados de precisar la forma en que se comunicarán los dispositivos de enrutamiento dentro de una red, una de sus principales funciones es compartir información entre equipos del mismo AS o entre dispositivos de enrutamiento de frontera en diferentes AS. Lo anterior se usa para generar y actualizar las tablas de enrutamiento con el fin de conocer la proximidad entre enrutadores [10].

Los protocolos de enrutamiento que se encargan de distribuir la información dentro de un dominio, se denominan Protocolos de Enrutamiento Intra-dominio (IGP:Interior Gateway Protocol) y se caracterizan por conocer la topología de red interna del AS al que pertenecen; por otro lado se encuentran los Protocolos de Enrutamiento Inter-domino (EGP: Exterior Gateway Protocol) los cuales transmiten y reciben información entre distintos AS y se caracterizan por no tener un conocimiento detallado de la topología de red de los AS vecinos [11].

Hoy en día, no es posible que un enrutador soporte tablas de enrutamiento con la cantidad de rutas que actualmente existen y de hacerlo, los tiempos de convergencia afectarían en gran escala el desempeño de las redes, haciendo ineficiente el proceso de enrutamiento. Dependiendo a las diferentes topologías de red y su escalabilidad, una forma de clasificación de los protocolos se basa en los criterios que utiliza el algoritmo para seleccionar la mejor ruta, esta decisión se fundamenta en el tipo de información que trasporta el protocolo y la forma en que cada enrutador actualiza su tabla de enrutamiento. Dicha clasificación se muestra a continuación indicando las ventajas y deficiencias de cada uno [11].

1.1.1 Protocolos de Vector Distancia

Los protocolos de vector distancia fueron utilizados en un principio por la compañía Xerox en su Protocolo de Información de Pasarela (GIP: Gateway Information Protocol) dentro de una arquitectura Sistemas de Redes Xerox (XNS: Xerox Network Systems). A inicios de 1969

ARPANET, se basó en los algoritmos de vector distancia desarrollados por R.E. Bellman, L.R. Ford Jr. y D.R. Fulkerson. En la actualidad los protocolos de enrutamiento de vector distancia más conocidos se encuentran el Protocolo de Información de Enrutamiento (RIP: Routing Information Protocol) en todas sus versiones, IGRP y EIGRP [12].

En el caso de un enrutador que usa el protocolo RIP, cuando ejecuta el mecanismo de selección de la mejor ruta, este crea su propia tabla de enrutamiento considerando tres variables entre las que se encuentran: la red destino, el próximo enrutador de salto y la distancia, la cual se entiende como el número de enrutadores para llegar al destino. Posteriormente, el enrutador envía a sus vecinos información relevante de la distancia que los separa entre sí y el indicador correspondiente con la ruta que debe seguir para alcanzarlo, la cual indica el próximo salto. Una vez todos los enrutadores han recibido la información de sus vecinos, actualizan sus tablas de enrutamiento y calculan si existe una mejor ruta, de ser así, el dispositivo comunicará esta posible ruta a los enrutadores vecinos [9] - [13].

Sin embargo, en sus comienzos los protocolos de vector distancia contaban con deficiencias muy marcadas entre las cuales se encuentran [9] – [14].

- ✓ **Tiempo de convergencia:** Es el tiempo trascurrido entre el momento en que se presentan cambios, sean estos en la topología de la red o en la configuración de la misma, y el momento en que los enrutadores actualizan sus tablas de enrutamiento frente a dichos cambios. Durante el tiempo de convergencia solo se trasmite información necesaria para actualizar las tablas de enrutamiento.

- ✓ **Bucles de enrutamiento:** Se presenta cuando los paquetes nunca llegan al destino quedándose la información saltando de un enrutador a otro. Las dos causas que generan bucles de enrutamiento son: el tiempo de convergencia lento y la contradicción de información entre posibles rutas; esta última se presenta cuando un enrutador recibe información por parte de dispositivos vecinos, acerca de una posible ruta, considerando que uno de ellos la considera como no accesible.

Para solucionar el problema de bucles de enrutamiento generados por cualquiera de las causas mencionadas anteriormente, se encuentran las siguientes [9] – [14]:

- ✓ **Horizonte dividido:** La información de enrutamiento no se envía al dispositivo vecino, al cual originalmente se le asocia la actualización; salvo que la información considere otra ruta viable al destino.

- ✓ **Envenenamiento de rutas:** Es una evolución a la solución de horizonte dividido; donde, en lugar de suprimir la ruta que se considera como inaccesible, ésta se agrega a un campo de la tabla de enrutamiento del dispositivo, el cual indica el correcto funcionamiento de la red a eventuales cambios topológicos de la misma. El objetivo es que los enrutadores vecinos actualicen sus tablas de enrutamiento incluyendo la ruta envenenada, para poder así descartarla como posible camino hacia un destino especifico.

- ✓ **Temporizador de espera:** Inmediatamente después de una actualización de la tabla de enrutamiento pone en marcha un temporizador, durante ese periodo de tiempo, no permiten cambios en los enrutadores que pudiesen afectar las rutas establecidas. Si el cambio es favorable, lo cual permite el acceso a una red que no lo tiene, la tabla de enrutamiento se

actualiza y elimina el temporizador. La red se considera inaccesible si al trascurrir el tiempo del temporizador no se da un cambio óptimo.

- ✓ **Uso de una única métrica:** Los protocolos de enrutamiento de vector distancia utilizan una sola métrica para determinar la mejor ruta, la más utilizada generalmente es el número de saltos. Esto ocasionaba conflictos con una de las soluciones propuestas al problema de los bucles en el enrutamiento, pues solo permite un máximo de 16 saltos, lo que implica considerar una ruta como inalcanzable. En redes grandes es un problema que amerita una rápida solución [15].

1.1.2 Protocolos de Estado de Enlace

El protocolo de estado de enlace nace en el año de 1979 para sustituir en ARPANET al protocolo de vector distancia que hasta ese momento fue utilizado para encaminar la información por internet. Posteriormente este protocolo se utilizó para el enrutamiento de tráfico intra-dominio [16].

Los enrutadores que operan con el protocolo de estado de enlace, proporcionan mediante una tabla la información referente al estado de los enlaces de la red, presentando si el segmento de red está o nó en funcionamiento, por medio de los Anuncios de Estado de Enlace (LSA: Link State Advertisement). Paralelamente, se generan las tablas que contienen información topológica de la red, denominadas Bases de Datos de los Estados de Enlace (LSD: Link State Database); estas tablas contienen todas las LSA que están dentro de un AS. Los dispositivos de enrutamiento utilizan el algoritmo Primero la Ruta más Corta (SPF: Shortest Path First) para construir su tabla de enrutamiento y determinar el mejor camino hacia el dispositivo destino, considerando como métrica el coste del enlace basado en el algoritmo de Dijkstra[1]. Por último y con el resultado arrojado por el algoritmo SPF, se crea un árbol de red lógico con las rutas más cortas, encabezándolo el dispositivo de enrutamiento [9] – [14].

Los protocolos de estado de enlace presentan características que los hacen atractivos al momento de elegir un protocolo de enrutamiento [14].

- ✓ **Actualización de los LSA:** Se actualizan únicamente cuando se presentan cambios topológicos en la red, por lo tanto consumen menos recursos de red.

- ✓ **Convergencia más rápida:** En el momento en que sucede un cambio topológico dentro de un dominio, los enrutadores actualizan inmediatamente sus tablas de enrutamiento.

- ✓ **Menos propensos a bucles de enrutamiento:** Por su amplio y anticipado conocimiento de la topología de la red, considerando una rápida convergencia del dominio.

- ✓ **No hay límite en el número de saltos de una ruta:** Los protocolos consideran otras métricas aparte del número de saltos, para determinar la mejor ruta, sin limitarse en un número máximo de saltos entre origen y destino.

- ✓ **Gestión de recursos:** Tanto el ancho de banda del enlace y el retardo pueden ser gestionados por el administrador de red inmediatamente después de elegir la mejor ruta.

[1] DIJKSTRA, un algoritmo utilizado para solucionar el problema de selección de ruta, tomando el camino de menor longitud desde un origen hasta un destino, por medio de grafos ponderados no dirigidos donde el costo de cada enlace es positivo.

- ✓ **Soporte para VLSM[2] y CIDR[3]:** Permite intercambiar información de las máscaras de subred, con el fin de tener una organización de direccionamiento jerárquico..

Como todo protocolo de enrutamiento posee desventajas que de ser manejadas adecuadamente, hacen de estos protocolos una herramienta ventajosa para el envío y recepción de información a un nivel intra-dominio. Entre las más importantes se encuentran:

- ✓ **Complejidad en el manejo de la información:** El protocolo debe generar un LSA para informar el estado de los enlaces, por otro lado crear un LSD para informar sobre la topología de red. Además de utilizar algoritmos de enrutamiento como SPF y por último, generar un Árbol de Expansión de costo Mínimo (MST: Minimum Spanning Tree) el cual construye lógicamente una topología de las rutas más cortas considerando los puertos de cada red destino.

- ✓ **Costo:** El protocolo requiere de más recursos computacionales, entre ellos la capacidad de memoria y mayor procesamiento.

- ✓ **Ancho de banda:** Se necesita disponer de un gran ancho de banda en el momento de trasmitir a todos los enrutadores la información contenida en los LSA, así como también en momentos de cambio de topología.

1.2 EL PROTOCOLO BGP

El protocolo de enrutamiento EGP fue creado en la década de los 80's y utilizado hasta la década de los 90's, para la comunicación y transporte de los datos entre distintos AS; sin embargo, no fue capaz de soportar el crecimiento exagerado de la red en tan poco tiempo, dando origen al desarrollo del Protocolo BGP, el cual se ha adaptado gradualmente a la expansión y exigencias de Internet; desde ese entonces se han conocido cuatro versiones, la última es la versión 4 (BGP-4), la cual fue aceptada por La Sociedad de Internet (ISOC: Internet Society), en enero de 2006 y convertida en el estándar RFC 4271; este protocolo ha sido modificado y adaptado por empresas privadas convirtiéndolo en un código privado, buscando soportar capacidades más complejas, debido al aumento del tráfico en Internet y al desarrollo de aplicaciones especializadas [17] – [18] - [19].

La función principal del protocolo de enrutamiento BGP es establecer un intercambio información entre diferentes AS, dicha información incluye una lista de los dominios por los cuales la información transita, la cual es suficiente para construir grafos de conectividad entre los AS, además de hacer cumplir las políticas de administración que se hayan implementado [17].

Para tal intercambio de información de enrutamiento entre dispositivos de frontera de cada AS, los dominios deben utilizar el protocolo BGP-4 como un lenguaje en común, es ahí donde el protocolo de enrutamiento antes mencionado juega un papel importante, debido a que permite la cooperación entre los enrutadores en el transcurso normal de sus procesos de intercomunicación.

[2] VLSM (Variable Length Subnet Mask): la Máscara de Subred de Tamaño Variable es una solución que se implementa cuando la asignación de direcciones IP llega a su límite.
[3] CIDR (Classless Inter-Domain Routing): Enrutamiento Inter-dominio Sin Clase, es el esquema de direccionamiento propuesto recientemente para Internet, el cual permite una asignación más eficiente de direcciones IP que el esquema de clases A, B y C.

BGP-4 provee una serie de mecanismos de enrutamiento entre dominios sin clase, entre los cuales se incluye un soporte para anunciar un rango de direcciones IP como destinos validos y eliminar así el concepto de "Clases" dentro de BGP. Asimismo, BGP-4 mediante sus mecanismos permite que se agregue rutas, incluso rutas hacia otros AS, por tal razón se cataloga como un protocolo inter-dominio [17].

Usualmente se hace referencia al protocolo BGP como un protocolo de Vector-Ruta, debido a que la información que ha sido transportada por este protocolo, reúne una serie de números que representa los AS que ha recorrido [5].

El protocolo de enrutamiento BGP-4 utiliza TCP como protocolo de transporte, asegurando de esta manera la confiabilidad de la transmisión de los datos (TCP es orientado a la conexión) y evitando implementar en BGP-4, mecanismos que ya están implementados en TCP como fragmentación, retransmisión, reconocimiento y secuenciamiento de paquetes, por consiguiente lo anterior hace de BGP-4 un protocolo eficiente en cuanto a que la información sea entregada a su destino de una manera segura antes de terminar la conexión [17].

A pesar de que el protocolo BGP-4 por sí solo no usa parámetros propios de la red como numero de saltos, ancho de banda o retardo en comparación con los protocolos de enrutamiento interno, si tiene la posibilidad de tomar decisiones de enrutamiento basadas en políticas de la red o de otras condiciones que pueden ser establecidas por el administrador de red [20].

El protocolo BGP se ha implementado de dos formas para comunicar los diferentes equipos que sirven para el enrutamiento ya sea dentro del mismo AS como hacia otros AS; en el caso de la comunicación intra-dominio, se implementó el Protocolo de Pasarela de Frontera Interior (iBGP: Interior Border Gateway Protocol) convirtiéndolos en vecinos BGP internos, a diferencia de los enrutadores ubicados en diferentes AS, los cuales implementan el Protocolo de Pasarela de Frontera Exterior (eBGP: Exterior Border Gateway Protocol) convirtiéndolos en vecinos BGP exteriores [20].

La información de enrutamiento intercambiada entre los equipos BGP de diferentes AS, se basa en el paradigma de reenvío de destino, el cual consiste en que un enrutador reenvía los paquetes basándose únicamente en la dirección IP destino que extrae de la cabecera [17].

Según el número de conexiones con otros AS y las respectivas políticas que los rigen, los dominios pueden ser catalogados en tres grupos [18] - [21]:

- ✓ **AS en Stub:** Es la configuración más sencilla, la cual presenta solo una conexión con otro AS, que usualmente será el ISP al que esté ligado. Por este AS circula solo tráfico local.

- ✓ **AS Multihomed:** Es el caso en el que un AS tiene más de una conexión con uno o más AS, ya sea por redundancia o por las configuraciones de la red; el tráfico que circula en estos dominios sigue siendo tráfico local.

- ✓ **AS Transit:** AS con varias conexiones que sirve como puente entre dos AS que no son vecinos, el trafico que maneja es de tipo *Transit*, sin embargo, las políticas de red que se establecen en estos sistemas, deciden qué tipo de trafico transportan y cual no.

1.2.1 Mensajes BGP

Ya sea que BGP-4 trabaje con uno o en su defecto con los tres tipos de AS, este protocolo maneja los siguientes mensajes para su funcionamiento en el intercambio de información de enrutamiento [17] – [18] – [20]:

- ✓ **Mensaje OPEN**: La función de este mensaje es iniciar la sesión entre vecinos BGP, se trata del primer mensaje que es enviado inmediatamente después de que una conexión TCP ha sido establecida y así acordar los parámetros de conexión.

- ✓ **Mensaje UPDATE**: Este mensaje es usado para transferir información de enrutamiento entre vecinos BGP del mismo o distintos AS, conteniendo en sus campos la información de los atributos para una ruta en particular como su longitud, enlaces retirados, entre otros y la lista de los AS que han intervenido en el procesamiento de datos, convirtiendo a este mensaje en un elemento esencial para que las tablas de enrutamiento siempre estén actualizadas.

- ✓ **Mensaje NOTIFICATION**: Este mensaje es utilizado para la detección o control de errores entre vecinos BGP, los cuales pueden presentarse por varias causas, ya sea por problemas en la configuración de los equipos, en las políticas implementadas, desacuerdos entre vecinos BGP, entre otras; cuando aparece este mensaje no se establece la sesión o se cierra si esta ya ha sido establecida, este tipo de mensajes son generados y entregados antes de finalizar la conexión TCP.

- ✓ **Mensaje KEEP – ALIVE**: Este mensaje tiene la función de notificar a los vecinos BGP que un dispositivo se encuentra activo o no, se envía periódicamente para tal fin.

De igual manera, el protocolo BGP-4 posee tres procedimientos funcionales que le permite detectar equipos, determinar si están al alcance, establecer una conexión e intercambiar datos con dichos elementos, los procedimientos son los siguientes:

- ✓ **Adquisición de vecino:** Proceso en el que un dispositivo de enrutamiento envía a otro una solicitud de participación, como posible ruta para el trasporte de información.

- ✓ **Detección de vecino alcanzable:** Inmediatamente después de establecerse la relación entre vecinos, se procede al intercambio de mensajes KEEP-ALIVE para mantener la comunicación entre dispositivos por un periodo de tiempo.

- ✓ **Detección de red alcanzable:** Cada dispositivo de enrutamiento conserva la información de enrutamiento, tanto con las redes alcanzables como con las mejores rutas. Cada vez que se presenta algún cambio topológico en la red, los enrutadores envían un mensaje UPDATE para notificar a sus vecinos BGP [17].

Se consideran vecinos a dos dispositivos de enrutamiento ubicados en la misma subred [18].

1.2.2 Atributos BGP

El protocolo BGP basa su proceso de decisión en los valores de sus atributos, a continuación se hace una explicación detallada de cada uno de ellos.

- ✓ **Atributo *ORIGIN:*** el atributo ORIGIN es indispensable para determinar el origen de la información de una ruta, asociada a un enrutador BGP. El byte de información no debe ser modificado por ningún otro enrutador BGP, y puede tomar valores entre 0 (información IGP), 1 (información EGP) o 2 (información incompleta) [17].

- ✓ **Atributo *AS_PATH:*** identifica los sistemas autónomos por los que ha transitado la información de enrutamiento almacenada en los mensajes UPDATE. Los componentes de esta lista pueden ser elementos de información conocidos como AS_SETS o AS_SEQUENCEs, que son asignaciones o secuencias respectivamente [5] - [17].

Cuando un enrutador BGP propaga una ruta aprendida a través de otro enrutador mediante un mensaje UPDATE, éste modifica el atributo AS_PATH basado en la localización del enrutador BGP al cual será enviada la ruta; dependiendo de la ubicación del enrutador respecto al AS, pueden presentarse dos casos [17]:

- ✓ Cuando el enrutador está dentro del dominio, el enrutador anunciante no debe modificar el atributo AS_PATH asociado con la ruta.

- ✓ Cuando el enrutador está fuera del dominio, el enrutador anunciante actualiza el atributo AS_PATH de la siguiente forma:

    1) Si el primer segmento de ruta del atributo es del tipo AS_SEQUENCE, el enrutador anexa su propio número de AS al último elemento de la secuencia.

    2) Si el primer segmento de ruta del atributo es del tipo AS_SET, el enrutador anexa al atributo AS_PATH un nuevo segmento del tipo AS_SEQUENCE, incluyendo su propio número de AS.

    3) Si el atributo está vacío, el enrutador crea un segmento de ruta del tipo AS_SEQUENCE, poniendo su número de AS dentro de ese segmento y colocándolo dentro del atributo AS_PATH.

Ahora, cuando un enrutador BGP origina una ruta entonces [17]:

- ✓ El enrutador iniciador, incluye su propio número de AS en el segmento de ruta del tipo AS_SEQUENCE, en el atributo AS_PATH de todos los mensajes UPDATE enviados a un enrutador BGP externo. En éste caso, el número de AS del enrutador iniciador será la única entrada del segmento de ruta, y su segmento de ruta será el único segmento en el atributo AS_PATH.

- ✓ El enrutador iniciador incluye un atributo AS_PATH vacío en todos los mensajes UPDATE enviados hacia los vecinos BGP internos (campo *Length* contiene el valor 0).

- ✓ **Atributo *NEXT_HOP:*** El atributo NEXT_HOP, define la dirección IP del enrutador que debe ser usado como el siguiente salto de la lista de destinos del mensaje UPDATE. El atributo NEXT_HOP se calcula de la siguiente manera [5] - [17]:

    1) Cuando se envía un mensaje a un enrutador BGP interno, si la ruta no es originada localmente, el enrutador debe modificar el atributo NEXT_HOP a menos que este haya sido configurado explícitamente para anunciar su propia dirección IP como NEXT_HOP.

Cuando se anuncia una ruta originada localmente a un enrutador BGP interno, el enrutador BGP debe usar la dirección de la interfaz del enrutador a través del cual, la red anunciada es alcanzable por el enrutador BGP como el NEXT_HOP. Si la ruta esta directamente conectada al enrutador, o si la dirección de la interfaz del enrutador a través de la cual, la red anunciada es alcanzable por el enrutador entonces este equipo BGP debe usar su propia dirección IP para el atributo NEXT_HOP (la dirección de la interfaz que es usada para alcanzar al enrutador BGP vecino).

2) Cuando se envía un mensaje a un enrutador BGP externo X, y este se identifica con un prefijo IP diferente respecto al enrutador local, entonces:

   a) Si la ruta anunciada fue aprendida de un enrutador BGP local o se originó localmente, el enrutador BGP puede usar la dirección de interfaz del enrutador interno a través de la cual, la red anunciada puede alcanzarse por el enrutador mediante el atributo NEXT_HOP, siempre que el enrutador X comparta una subred común con esta dirección.

   b) Por otra parte, si la ruta anunciada fue aprendida de un enrutador BGP externo, el enrutador puede usar una dirección IP de algún enrutador adyacente (conocido a través del atributo NEXT_HOP recibido) que el mismo sistema utiliza para calcular rutas locales en el atributo NEXT_HOP, siempre que el enrutador X comparta una subred común con dicha dirección.

   c) De otra forma, si el enrutador BGP externo a través del cual está siendo anunciada la ruta comparte una subred común con una de las interfaces del enrutador BGP anunciado, el enrutador puede usar la dirección IP asociada con dicha interfaz en el atributo NEXT_HOP.

   d) Si no se cumple ninguna de las condiciones anteriores, el enrutador BGP debe usar en el atributo NEXT_HOP, la dirección IP de la interfaz que el enrutador utiliza para establecer la conexión BGP con el enrutador X.

3) Cuando se envía un mensaje a un enrutador BGP externo X, y dicho enrutador se encuentra a múltiples saltos del enrutador local, entonces:

   a) El enrutador puede configurarse para propagar el atributo NEXT_HOP. En este caso, cuando se anuncia una ruta que el enrutador ha aprendido de uno de sus pares, el atributo NEXT_HOP de la ruta anunciada es exactamente el mismo que el atributo NEXT_HOP de la ruta aprendida (el enrutador BGP no modifica el atributo NEXT_HOP).

   b) Por defecto, el enrutador BGP debe usar la dirección IP de la interfaz que el enrutador utiliza en el atributo NEXT_HOP para establecer la conexión BGP con el par X.

Normalmente, el atributo NEXT_HOP se escoge de tal forma que sea elegida la ruta más corta disponible. La dirección del siguiente salto, es determinada ejecutando una operación recursiva de *LOOPBACK*[4] para la dirección IP en el atributo, usando los contenidos de la tabla de enrutamiento, seleccionando una entrada si existen múltiples entradas con igual costo [17].

[4] LOOPBACK: Es un tipo especial de interfaz que le permite hacer conexiones consigo mismo siendo una interfaz virtual, es decir, no existe físicamente en el equipo, sin embargo realiza las funciones de una interfaz normal [23]

- ✓ **Atributo *MULTI_EXIT_DISC:*** El atributo MULTI_EXIT_DISC está pensado para ser usado en enlaces externos, con el fin de diferenciar entre múltiples puntos de entrada o salida para llegar a un mismo AS. El valor de este atributo es llamado *métrica*. El punto de salida con la menor métrica debe preferirse. Si el atributo se recibió de un protocolo EBGP, éste puede propagarse a través de un protocolo IBGP hacia otros enrutadores BGP dentro del un dominio; sin embargo, si este atributo se recibe de un vecino BGP, éste no debe propagarse hacia otros enrutadores en otros dominios.

Un enrutador BGP basado en su configuración local, puede cambiar el valor del atributo recibido desde un EBGP, si es así, dicha alteración debe hacerse antes de determinar el grado de preferencia de la ruta y antes de realizar la selección de ruta (Fases 1 y 2 del proceso de decisión) [17] - [22].

- ✓ **Atributo *LOCAL_PREF:*** El atributo LOCAL_PREF es un atributo que debe incluirse en todos los mensajes UPDATE que un enrutador BGP envía a otros pares BGP internos. Un enrutador BGP, debe calcular el grado de preferencia para cada ruta externa basado en una política de configuración local, e incluyendo el grado de preferencia cuando se anuncia una ruta a sus pares internos. El mayor grado de preferencia es el elegido; además, un enrutador BGP usa el grado de preferencia aprendido a través de éste atributo en su proceso de decisión [5].

  Por otra parte, un enrutador BGP no debe incluir este atributo en los mensajes UPDATE que él envía a sus pares BGP externos. Si dicho atributo está contenido en un mensaje UPDATE recibido de un par externo, entonces este atributo debe ser ignorado por el enrutador receptor [5].

- ✓ **Atributo *ATOMIC_AGGREGATE:*** Cuando un enrutador BGP agrega muchas rutas con el propósito de anunciarlas a un par BGP en particular, el atributo AS_PATH de la ruta agregada, normalmente incluye un AS_SET formado por el conjunto de AS de los cuales fue formada la agregación. Si dicha agregación excluye al menos algunos de los números de AS presentes en el AS_PATH de las rutas que son agregadas como resultado del fallo del AS_SET, la ruta agregada, cuando es anunciada al par, debe incluir el atributo ATOMIC_AGGREGATE. De esta forma, un enrutador BGP que recibe una ruta con el atributo ATOMIC_AGGREGATE, no debe remover el atributo cuando propaga la ruta hacia otros enrutadores BGP [17].

- ✓ **Atributo *AGGREGATOR*** Un enrutador BGP que realiza la agregación de rutas puede o no adicionar éste atributo, el cual contiene únicamente su propio número de AS y su dirección IP. Cabe anotar que la dirección IP debe ser la misma que la del identificador BGP del enrutador [17].

1.2.3 Proceso de Enrutamiento con el protocolo BGP-4

Cuando existen múltiples rutas con la misma longitud hasta un destino en común, BGP basa su proceso de decisión en los valores de sus atributos. El siguiente proceso resume como BGP selecciona la mejor ruta [5]:

1. Como primer criterio, se elige la ruta con el mayor valor de LOCAL-PREFERENCE de acuerdo a las políticas de tráfico entrante, la cual se envía a otros enrutadores vía iBGP.

2. Si el valor de LOCAL-PREFERENCE no estuviese asignado, o fuera igual en todos los casos, se prefieren las rutas con menor número de sistemas autónomos entre origen y destino, por lo general es la opción por defecto del protocolo BGP-4.
3. Si el valor de AS_PATH es igual en todos los casos, se escoge el menor valor del atributo ORIGIN (Una ruta aprendida de un EGP posee un mayor valor del atributo ORIGIN que una ruta IGP).
4. Se selecciona la ruta con menor valor de MED; solo es posible comparar aquellas que son aprendidas desde un mismo AS vecino. Si una ruta no posee MED se le asigna el menor valor posible.
5. Se elige eBGP sobre iBGP: Se prefieren las rutas aprendidas por eBGP que las aprendidas por iBGP, debido a que la información es más directa hacia el AS destino.
6. Posteriormente se escoge la métrica IGP más baja: Se eligen las rutas con menor valor de métrica IGP para llegar al siguiente salto. Esto permite que cada dispositivo elija el punto de salida "más cercano".
7. Si todos los puntos anteriores no son satisfactorios para una selección de ruta, se procede a seleccionar el Identificador más bajo: Según la dirección IP, se prefiere la ruta con el menor Identificador de enrutador. Con esta comparación se acaba con la igualdad en los atributos de las otras posibles rutas.

1.3 INGENIERÍA DE TRÁFICO

Las telecomunicaciones han tenido un avance importante en cuanto a la convergencia de los backbones que trasportan información ya sea de voz o datos soportados sobre redes IP, como también en la convergencia de servicios percibidos por el usuario final, sin dejar de lado la QoS, indispensable para determinar el desempeño de una red.

La QoS es un parámetro fundamental dentro de las telecomunicaciones, el cual indica el optimo desempeño de la red respecto a variables definidas como el retardo, jitter, pérdida de paquetes, entre otras; dichas variables son intrínsecas de la red y se asocian a los protocolos y dispositivos utilizados en todo el sistema. Existen otras variables que deben considerarse cuando se habla de QoS y son aquellas que no dependen de la arquitectura de red sino de factores externos, entre las cuales se encuentran, el soporte técnico, la operabilidad y la seguridad [2].

Las redes de telecomunicaciones actuales soportan gran variedad de servicios, es por esto que se hace necesario que los Proveedores de Servicio de Internet (ISP: Internet Service Provider) cuenten con herramientas de gestión y sus equipos con protocolos de enrutamiento que permitan optimizar los recursos de sus redes, además de determinar las mejores rutas para el envió y recepción de tráfico [24].

La Ingeniería de Tráfico es una rama de la Ingeniería de Telecomunicaciones que se encarga de optimizar los recursos de la red para mejorar el desempeño de la misma; esta incluye mecanismos que permiten medir, caracterizar, modelar y controlar el tráfico en Internet. La TE tiene como objetivo optimizar y hacer uso eficiente de los recursos de la red de una forma que estos no se saturen mientras que otros están subutilizados [24].

Como objetivo general, la TE busca reducir la congestión, sin dejar de lado la optimización de recursos. La congestión es un fenómeno que afecta en una forma abrupta el desempeño de la red, en estos casos la solución más fácil pero a la vez más costosa y por tanto menos favorable es el aumento de capacidades a los dispositivos de red [24].

Los objetivos de la TE consideran mejorar continua e iterativamente los procesos de rendimiento de la red, además de estar a la vanguardia de las nuevas tecnologías que permitan cumplir con dichos objetivos. Por otro lado, la TE se encuentra dividida en dos partes de acuerdo a sus alcances, estas son [25]:

- ✓ **TE Orientada a tráfico:** Se basa en el mejoramiento de la Calidad de Servicio en el flujo de información, minimizando el retardo, la pérdida de paquetes y maximizando el desempeño para dar cumplimiento a los acuerdos de nivel de servicio.

- ✓ **TE Orientada a recursos:** Se limita a aspectos relacionados con la optimización de los recursos, dentro de los cuales se encuentra el ancho de banda y la capacidad de los buffers.

Cumplir con estos objetivos en redes pequeñas que realizan trasporte de información a nivel intra-dominio no es tan complicado considerando que normalmente la infraestructura de red se encuentra sobredimensionada a los requerimientos de tráfico, lo que implica que no se va a presentar una congestión notable en los enlaces de la red. Por otro, el conocimiento de la topología interna de AS se conoce gracias a que estos utilizan protocolos de enrutamiento de estados de enlace que hace que los dispositivos de enrutamiento compartan una imagen de la topología de la red [26].

En el caso contrario, agregar capacidades de TE a un enrutamiento inter-dominio no es tan fácil ya que se debe tener en cuenta las políticas de enrutamiento y las configuraciones de los protocolos de enrutamiento utilizados para enviar información a un destino especifico, en busca de reducir el retardo y la congestión sin afectar el desempeño de la red. Por otro lado, la topología de internet complica más el enrutamiento inter-dominio pues no puede considerar todas las rutas posibles para alcanzar un destino, ya que los protocolos de enrutamiento de vector distancia utilizados en este contexto no lo permiten [27].

Sin embargo se han creado mecanismos que permiten adicionar capacidades de TE al proceso de enrutamiento, entre las cuales se encuentran [28]:

- ✓ **Enrutamiento Explícito:** Técnica en la que el administrador de red visualiza los posibles enlaces para crear salto a salto una ruta desde un nodo origen a un nodo destino. El enrutamiento explícito no utiliza un algoritmo de enrutamiento, simplemente se basa en la decisión del administrador de red para seleccionar la ruta que se desee [24].

- ✓ **Balanceo de Carga:** Mecanismo que permite redistribuir el tráfico hacia un destino a través de las diferentes rutas existentes. El balanceo de carga es uno de los componentes de la TE que permite optimizar la utilización de los recursos de la red, evitando la congestión y aumentando el rendimiento [29].

- ✓ **Enrutamiento Basado en Restricciones (CBR: Constraint Based Routing):** El enrutamiento basado en limitaciones es una técnica fundamentada en el uso de algoritmos de enrutamiento, los cuales seleccionan una ruta que satisface limitaciones de tipo administrativo (políticas de enrutamiento) o limitaciones en cuanto a servicios; estas permiten reducir costos, balancear la carga o mejorar la seguridad. Además, la ruta seleccionada cuenta con características especiales en cuanto a la reserva de recursos [30].

Como se menciona en la sección anterior, BGP es el protocolo utilizado actualmente para soportar el tráfico inter-dominio en Internet. Una característica importante de BGP es que permite definir dentro de un dominio, políticas de enrutamiento para la selección de la mejor ruta de acuerdo a las necesidades y requerimientos del administrador de red. Una vez establecidas dichas políticas, los dispositivos de enrutamiento intercambian sus mensajes con la información de ruta por la cual se van a enviar los paquetes hacia su destino. Sin embargo, aunque BGP selecciona "la mejor ruta", únicamente contempla como prioridad la ruta que posea el menor valor de costo total para alcanzar dicho destino, sin considerar características propias de los enlaces como ancho de banda o congestión. En consecuencia la TE a nivel inter-dominio se considera compleja por no tener un conocimiento detallado de las políticas de enrutamiento y de la topología de los AS vecinos [3] – [31].

En consecuencia, se han desarrollado estudios enfocados a la optimización del protocolo de enrutamiento BGP-4, los cuales pretenden incluir parámetros o métricas que cuenten con criterios para la selección de "la mejor ruta" en el proceso de intercambio de información entre un origen y un destino específico. En el siguiente capítulo se hace un análisis para determinar cual parámetro y métrica se pueden incluir para agregar capacidades de ingeniería de tráfico al protocolo BGP en busca de reducir la congestión en redes IP [3].

1.4 CONGESTIÓN

La congestión es un fenómeno que puede definirse de diferentes formas, sin embargo, su efecto es el mismo independientemente del punto en que se presente; una aproximación a la definición puede interpretarse como la pérdida de información ocasionada por un exceso de tráfico de la misma en una red; es decir, cuando el tráfico inyectado sobrepasa la capacidad del canal.

Este aspecto representa uno de los problemas más críticos en una red de telecomunicaciones, el cual es originado por diversos factores como la existencia de computadores con una memoria insuficiente, que presentan una saturación en sus buffers de entrada o salida debido a una tasa de transmisión elevada y por ende la información no alcanza a ser procesada, o porque los nodos de la unidad de control de procesamiento, son incapaces de manejar una gran cantidad de tráfico obligándolos a descartar datos de sus buffers, entre muchos otros [32].

Una causa interesante según algunos autores, es el efecto de retroalimentación que tiene la congestión, en cuanto a que conduce inevitablemente a la pérdida de paquetes de información, viéndolo como indicador de este fenómeno; dicha pérdida de información ocasiona retransmisiones, produciendo un incremento en el tráfico de datos en la red y causando a su vez retardos excesivos, ocasionando que las colas de los enrutadores lleguen a su máxima capacidad, comprometiendo el desempeño de los equipos y contribuyendo de igual forma a que la congestión se presente en mayor medida [32] - [33].

Como respuesta a este inconveniente, se han creado mecanismos que buscan minimizar los problemas de congestión, los cuales buscan enfrentar la congestión en un momento dado, desde varios puntos, las soluciones pueden ser pasivas o activas [32].

Las soluciones en bucle abierto o soluciones pasivas, son las que buscan prevenir el fenómeno de congestión en el momento del dimensionamiento y posterior diseño de la red, basándose en la modificación de variables de diseño que están directamente relacionadas

con este fenómeno; a nivel de enlace con variables de diseño de temporizadores, control de flujo, políticas de retransmisiones, de descartes y almacenamiento de paquetes que no llegan en orden; a nivel de red, con variables relacionadas con circuitos virtuales, algoritmos de enrutamiento, tiempo de vida de los paquetes y políticas de colas, servicio y descarte de paquetes, por último a nivel de transporte, con las variables relacionadas con los enlaces entre sistemas o dispositivos finales [32].

El segundo mecanismo que se plantea, consiste en procesos que actúan en el momento preciso en el que se presenta el inconveniente, denominándose soluciones en bucle cerrado o soluciones activas, las cuales se desarrollan en tres etapas, la primera es una monitorización de parámetros como el estado de enlaces y de buffers, porcentaje de descartes, numero de retransmisiones, entre otros; la segunda etapa es la reacción para el envío de información a los puntos necesarios, por medio de paquetes especiales que tienen prioridad sobre el tráfico normal de datos en la red, por transportar alertas de congestión, y la tercera etapa se refiere al ajuste del sistema, con medidas que deben considerarse en el momento de reducir la velocidad de transmisión, el control de acceso y el descarte de paquetes que están en cola, esperando ser atendidos [32].

1.4.1 Pérdida de Paquetes como Indicador de Congestión

La congestión, genera distintos inconvenientes en una red, uno de ellos es la pérdida de información, ya sea porque el tiempo de vida del paquete ha terminado o por que el enrutador lo descarta al presentarse una saturación en sus buffers de entrada o salida, ocasionando así nuevos problemas, comprometiendo en un alto grado el desempeño y los recursos de un sistema [32].

La mayoría de los protocolos de enrutamiento usados actualmente asumen que la pérdida de paquetes que se registre en una red, es un indicador de congestión que se presenta en la misma. Este factor, es un dato importante para las aplicaciones que actualmente basan su funcionamiento sobre TCP, las cuales toman ciertas medidas para hacer frente a un incremento de congestión, como la reducción de tasa de transferencia, por medio de la reducción del tamaño de la ventana de transmisión [34].

La propuesta de este proyecto, es tomar una medida frente a la congestión que se presenta en los diferentes caminos que conectan a uno o más AS, seleccionando cuál de estas rutas es la más idónea para enviar la información hacia un destino.

Un enrutamiento adecuado se considera indispensable en el proceso de intercambio de información, sin embargo no siempre se toman las mejores decisiones de enrutamiento, lo que puede ocasionar pérdida de información, caso critico en redes consideradas de alta prioridad en el trasporte de información tales como las bancarias y de seguridad. Ahora bien, por los requerimientos de las aplicaciones en tiempo real y las exigencias de los usuarios, es indispensable que los Proveedores de Tecnología como los ISP, ofrezcan servicios de alta QoS, que les permita brindar confiabilidad en el trasporte de información.

Gracias al análisis teórico, se logra establecer una base de conocimiento acerca del funcionamiento del protocolo de enrutamiento BGP-4, consideraciones generales de TE y cómo se relacionan congestión y pérdida de paquetes, esto será utilizado en el siguiente capítulo para lograr el desarrollo en la investigación.

CAPITULO II: ADAPTACIONES DEL PROTOCOLO BGP BAJO CONSIDERACIONES DE TE Y QoS

En la actualidad se pretende optimizar el desempeño de una red, considerando el proceso de enrutamiento y el control de tráfico, mediante estudios relacionados con modificaciones a protocolos de enrutamiento para agregarles capacidades de ingeniería de tráfico [3].

Las adaptaciones e implementaciones sugeridas a los protocolos de enrutamiento, se presentan precisamente porque estos no cuentan con capacidades de ingeniería de tráfico, que les permitan censar los enlaces con el objetivo de detectar la existencia de problemas que afecten el desempeño de la red; considerando parámetros como congestión, ancho de banda, retardo, jitter, entre otros. El problema de congestión se ha enfrentado a nivel hardware, aumentando las capacidades de los distintos dispositivos de red con el inconveniente de los altos costos que acarrean. Asimismo, las soluciones software ofrecidas, se limitan solo a la implementación de herramientas de gestión para el nivel de aplicación, de algoritmos más eficientes para el nivel de red y de políticas de funcionamiento y variables de diseño para el nivel de enlace.

La optimización de los protocolos de enrutamiento, busca reducir la congestión de tráfico mediante el uso eficiente de los recursos de la red; para cumplir con dicho propósito, se hace necesario aplicar políticas que consideren los parámetros de red junto con sus métricas de enrutamiento, de tal forma que las decisiones para el envío de información se tomen de acuerdo al estado de los enlaces disponibles en una red [4].

Es de suma importancia, implementar mecanismos que permitan aprovechar al máximo los recursos de la red, para no incurrir en gastos adicionales de infraestructura. Desafortunadamente, optimizar el enrutamiento inter-dominio es bastante complejo debido a que los protocolos no brindan información específica sobre los recursos propios de la red [4].

El presente capitulo, define una base conceptual de las métricas de enrutamiento utilizadas en el mejoramiento del proceso de decisión para intercambiar información entre diferentes AS, así como también de los mecanismos de enrutamiento basados en BGP, los cuales agregan capacidades de TE en busca de optimizar los recursos propios de la red; además, se plantea una solución frente al problema de decisión que presentan los enrutadores BGP para el intercambio de información entre dominios, la cual se basa en la adaptación del protocolo BGP-4 considerando la congestión como parámetro de red, la métrica como variable que permite identificar la mejor ruta entre las posibles y el atributo propio de BGP que define el grado de preferencia de la ruta para el envió de información de un origen a un destino especifico.

2.1 MÉTRICAS DE ENRUTAMIENTO

Cuando se presentan cambios en la topología de la red, los enrutadores reciben de sus vecinos información de posibles nuevas rutas, actualizan sus tablas de enrutamiento y asignan un valor de métrica que permita identificar la mejor ruta para el trasporte de información, valor que debe estar dentro del rango permitido, según la configuración del protocolo de enrutamiento, para que el destino no sea considerado como inalcanzable [13].

El protocolo de enrutamiento BGP-4, basa su proceso de decisión en el menor valor de métrica establecida por el administrador de la red, el cual se almacena en las tablas de enrutamiento de cada dispositivo y representa una variable que permite al enrutador, determinar la mejor ruta posible para el envío de información, aunque en la mayoría de los casos la decisión no es la mejor. En la tabla 1 se presenta un resumen de las métricas comúnmente utilizadas por los diferentes protocolos de enrutamiento [35].

Tabla 1 Métricas de Enrutamiento más Utilizadas

Métrica	Descripción
Número de Saltos	Número de enrutadores por los que debe pasar un paquete hasta llegar al destino.
Ancho de banda	Capacidad del enlace para soportar determinado tráfico.
Carga	Frecuencia en el uso del enlace y número de paquetes que transitan por él.
Confiabilidad	Determina el número de bits de error ocurridos en un enlace.
Costo del Enlace	Valor que se establece por el Administrador de Red para determinar la preferencia por una ruta.
Retardo	Indica el tiempo que se demora un paquete en trasladarse de un origen a un destino.

2.2 INTRODUCCIÓN A LA OPTIMIZACIÓN DEL PROTOCOLO BGP

En la búsqueda de mejorar cada vez más el proceso de intercambio de información entre diferentes AS, se han implementado mecanismos que de una u otra forma han contribuido con el correcto uso de los recursos de la red.

El protocolo BGP-4 optimizado basa sus decisiones de enrutamiento en políticas definidas por los administradores de red, estas pueden ser comerciales, administrativas, de tráfico, geográficas, entre otras, las que deben ser cumplidas, lo que conlleva a la preferencia de un enrutador de entrada o salida del dominio por encima de otro.

Una vez implementado el protocolo BGP-4, el proceso de enrutamiento básico comienza cuando un dispositivo BGP recibe y actualiza sus tablas de enrutamiento a partir de información exclusiva de dicho proceso, la cual es enviada por sus vecinos. Antes de continuar describiendo el proceso de enrutamiento, cabe recordar que BGP-4, siempre y cuando no aplique políticas al tráfico entrante proveniente de un mismo o de diferentes dominios, considera únicamente el número de sistemas autónomos consecutivos para determinar la mejor ruta. La optimización del protocolo se fundamenta en la aplicación de políticas mencionadas anteriormente, basándose en la manipulación de los atributos propios de BGP-4, para descartar así rutas no deseadas. Inmediatamente después, el algoritmo de decisión selecciona la mejor ruta; en el caso de que estas presenten características iguales, su decisión dependerá de los criterios de desempate mencionados en el ítem 1.2.3 Proceso de Enrutamiento del Protocolo BGP-4 [17] – [36]:

Después de aplicar los criterios de decisión para la selección de la mejor ruta, se procede a aplicar políticas de tráfico saliente y determinar si anuncian o no la mejor ruta a sus vecinos BGP. Cabe anotar que el último criterio se evalúa siempre y cuando el criterio anterior haya sido evaluado en 2 o más rutas posibles. La figura 2, indica de manera general como en el proceso de enrutamiento son utilizados los atributos y la forma como se interpretan dentro del proceso de decisión de la mejor ruta [35] - [36].

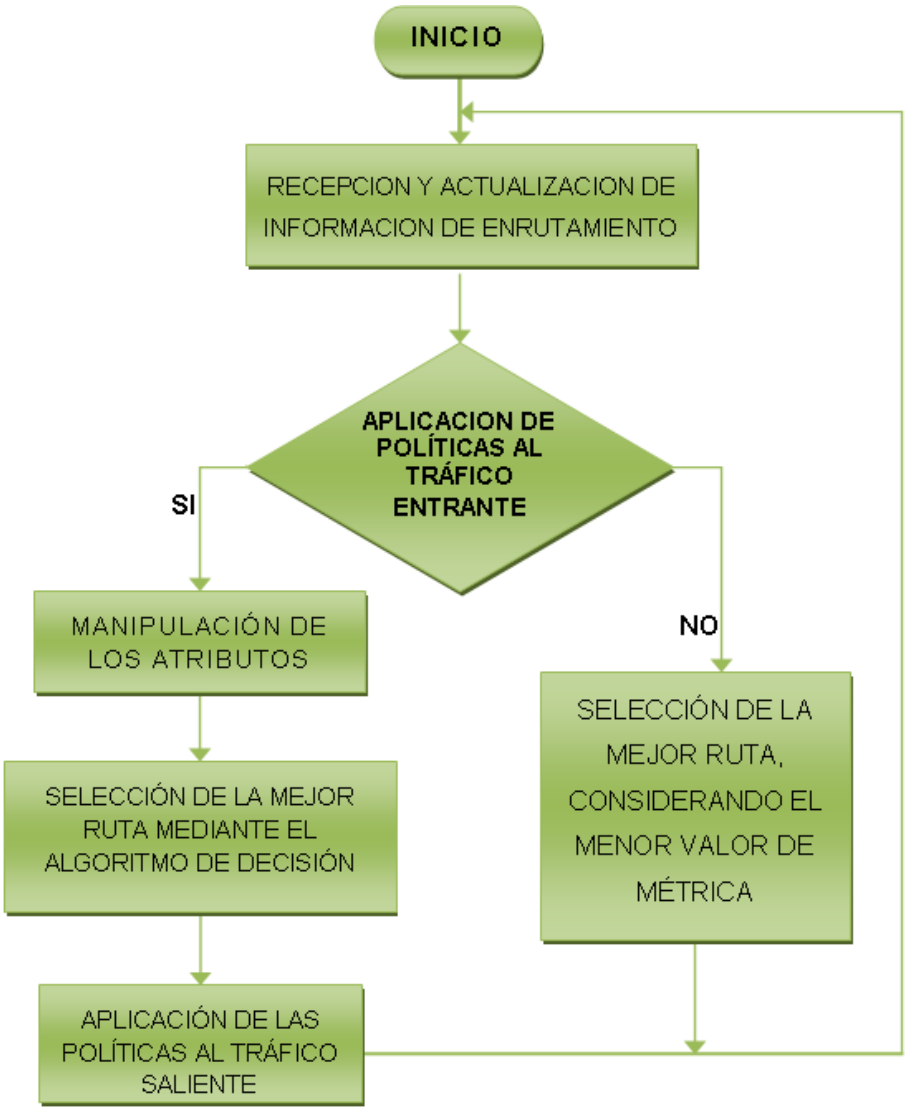

Figura 2 Proceso de Enrutamiento Básico de BGP

2.3 MECANISMOS ACTUALES QUE IMPLEMENTAN CAPACIDADES DE TE CON EL PROTOCOLO BGP-4.

Se han realizado varias propuestas para mejorar el proceso de enrutamiento, basándose en modificaciones al protocolo de enrutamiento BGP-4, las cuales se enfocan en la manipulación de sus atributos y/o recurriendo a estrategias que permiten controlar el flujo del tráfico, ya sea a

nivel intra-dominio como a nivel inter-dominio. Dentro de los mecanismos se encuentra una adaptación al protocolo, considerando el atributo Communities, desarrollado por Cisco Systems en sus equipos y plataformas, para ofrecer un mejor servicio a sus clientes. A continuación se citan las propuestas que han sido publicadas en los artículos correspondientes a dichas modificaciones.

2.3.1 Communities

Algunos ISP han implementado el uso del atributo opcional transitivo Communities, para realizar una redistribución de sus rutas y así ofrecer un mejor servicio a sus clientes; el valor de este atributo se adhiere a las rutas con el fin de realizar una segmentación de la red, por ejemplo para asignar un código por ciudad o por zona.

Sin embargo, el uso del atributo opcional transitivo fue desarrollado por la empresa Cisco Systems y por tanto, es de uso único y exclusivo de sus equipos y plataformas [37].

El atributo opcional transitivo Communities, permite realizar una segmentación de la red, agrupando destinos dentro de un mismo rango llamado “Comunidad”, la cual reúne un grupo de rutas con características comunes o que según las políticas administrativas de la red, deberían recibir un tratamiento diferente que las demás rutas por parte de los equipos BGP de frontera [37].

La organización de este atributo se compone por uno o más números de 32 bits cada uno de los cuales, 16 bits de mayor orden representan el sistema autónomo, los restantes 16 bits que se entienden como de menor orden, definen como debe ser tratado el atributo [37].

Este atributo se cataloga como uno de los mecanismos de control de flujo entrante a un dominio, y se comporta de tal forma que, establecidas las comunidades dentro del dominio, en el momento de recibir algún tráfico por los puntos de entrada, se les puede dar un trato diferencial dependiendo de la información que contenga el atributo; por lo que aumentaría la efectividad en el control y el manejo de la información recibida y la selección de los puntos más adecuados para su recepción [37].

Para el manejo de este mecanismo, se cuenta con tres comunidades, las cuales son:

- ✓ **NO_ANNOUNCE:** permite que las rutas no sean anunciadas a vecinos BGP particulares.
- ✓ **PREPEND:** permite agregar uno o más AS en particular al AS_Path cuando se realizan los anuncios de ruta a los vecinos BGP.
- ✓ **CHANGE_PREF:** permite asignar un valor al atributo Local_Preference en el AS que recibe la ruta.

Entonces, las ventajas que trae consigo este atributo son varias, permite no solo transferir información de enrutamiento a los demás dominios si no que envía esta información a enrutadores BGP de los AS lejanos, aprovechando la información que lleva el atributo para diferenciar rutas y tomar mejores decisiones frente a ellas.

Se propone como ejemplo la *Figura 3*, donde se puede apreciar que el AS1 tiene dos rutas para enviar su información hacia AS5, dichas rutas deben atravesar otros dominios para

alcanzar su destino; con el funcionamiento estándar del protocolo BGP-4, el AS1 podría identificar características de las dos rutas por estar conectado directamente a ellas con el fin de seleccionar uno de estos enlaces, sin embargo, en este proceso no podría obtener información de los dominios que intervienen en el envío de su información hacia el AS5, por lo cual la decisión solo dependerá de los enlaces contiguos.

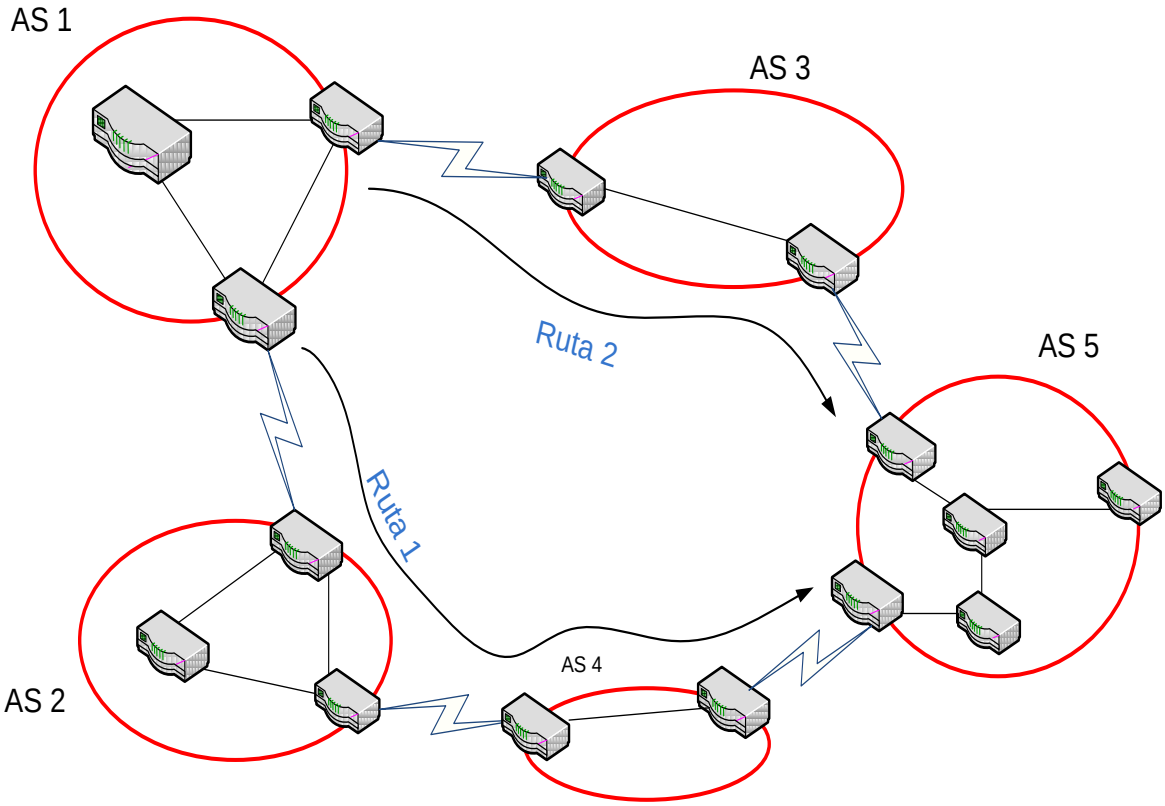

Figura 3 Mecanismo que hace uso del Atributo Communities

Con el atributo Communities, se podrían enviar las características relevantes de los dominios que intervienen entre el origen y el destino, por lo tanto el AS1 tendría más información para seleccionar la ruta más idónea en el envío de sus datos.

El atributo Communities fue desarrollado por Cisco Systems y se reservan su uso para los equipos que ensamblan y distribuyen, no hace parte del estándar del protocolo BGP-4, por tanto el acceso a la información de este atributo es mínima y su utilización de carácter privado aunque son muchas las ventajas que ofrece su implementación respecto al proceso de enrutamiento [37].

2.3.2 Otros Mecanismos

En la tabla 2, se presenta la información de otros mecanismos, teniendo en cuenta sus ventajas y desventajas.

Tabla 2 Otros Mecanismos para Optimización

Mecanismo y descripción	Ventajas	Desventajas
Único Punto de Salida (SES: Single Egress Selection), basándose en el método de balanceo de carga, este mecanismo selecciona un enrutador de frontera como único punto de salida para cada AS, el cual recibe todo el tráfico generado por el dominio origen u otros dominios que no alcancen directamente al AS destino [38].	- Permite asignar prioridades al tráfico. - Es más fácil controlar el tipo de tráfico que sale del dominio.	- El tráfico dentro del dominio podría aumentar considerablemente. - Se generan cuellos de botella al enviar una gran cantidad de tráfico por un solo punto de salida. - El enrutador BGP de salida, tendrá que procesar mucha más información y está más proclive a bloquearse.
Múltiples Puntos de Salida (MES: Multiple Egress Selection) permite que se utilicen varios enrutadores BGP de salida de un dominio, para el tráfico que se dirige hacia un AS en particular [38].	- Al haber más puntos de salida, el balanceo de carga permitiría dar un mayor margen de trabajo a los enrutadores de salida antes de bloquearse. - Se deben establecer las mismas políticas de tratamiento de tráfico en cada enrutador de salida para evitar contradicciones entre ellos.	- El artículo "Optimal Configuration for BGP Route Selection" que lo propone, solo considera un caso de escenario de red por proximidad geográfica, no hay registros de estudios en otros escenarios. - Su estudio solo contempla puntos de salida y no un tratamiento al tráfico, por tanto, no representa una solución permanente a los inconvenientes de congestión.
Discriminador de Múltiple Salida (MED: Multi Exit Discriminator), es un método que a partir de un atributo del protocolo de enrutamiento BGP selecciona un enrutador como un único punto de entrada al AS, este método es comúnmente utilizado como objeto de negociación entre dos dominios; otro atributo que sirve para este fin es AS_PATH, el cual cambia su valor, para informar al dominio origen que el AS destino esta mas lejos de lo que realmente se encuentra [38].	- La información que intente ingresar al dominio, tendría un mayor control, por ser un único equipo encargado de supervisarla y darle un tratamiento especial. - Se evitaría que tráfico que no tuviera un destino en específico dentro del AS, entre al dominio innecesariamente. - Al solo ser implementado por un dominio que presente varios enlaces hacia otro, garantiza que en caso de falla en el enrutador dispuesto como entrada, lo pueda sustituir otro enrutador.	- Los buffers del equipo de entrada estarían más propensos a saturarse y ocasionar que los datos se pierdan al no recibirse de una manera rápida y eficaz. - Al tener solo un punto de entrada al dominio, este generaría congestión en el enlace inter-dominio. - Solo puede ser implementado por un dominio que presente varios enlaces hacia un AS en común
Enrutamiento de Papa Caliente (HPR: Hot Potato Routing) es quizás el mecanismo más utilizado en las redes de datos, por su implementación no solo con el protocolo BGP, si no con protocolos como OSPF; su objetivo consiste en evacuar el	- Es un método sencillo para descongestionar los dominios y cursar el tráfico hacia otros AS más rápidamente. - No exige mayor configuración en sus equipos, ya que el mismo protocolo BGP incorpora	- El administrador, debe establecer todas las políticas de red manualmente como puntos de entrada y salida, llegando a ser un trabajo arduo y demorado. - Aunque el mecanismo HPR tome la mejor decisión de enrutamiento a nivel intra-dominio, no significa que tome la decisión más acertada en

tráfico que se procesa dentro del dominio al exterior, por la ruta que presente un menor costo, encontrando el punto de salida más cercano [38].	este sistema como predeterminado.	la selección de ruta hacia otro AS. - No considera más parámetros de red, basándose solo en el costo asignado a cada salto, generando inconvenientes como retardos, pérdida de datos, entre otros.
Método de menor costo IGP: consiste en asignar valores IGP a los enlaces dentro de un dominio, dichos valores obedecen a diversos factores o en su defecto a una asignación arbitraria del administrador de la red y es considerado por el protocolo BGP para seleccionar la ruta que presente un menor valor total de costo IGP, para cursar el tráfico hacia el punto de salida del AS [38].	- Es el método que quizás combate mejor el problema de la congestión intra-dominio y pretende contribuir a reducir el mismo problema a nivel inter-dominio. - Si las asignaciones de los costos IGP de los enlaces están relacionadas con las rutas de salida de un dominio, podría seleccionar la mejor ruta evitando problemas de congestión, retardos, pérdidas, entre otros. - Este mecanismo es atractivo para convenios comerciales a nivel económico para diferentes dominios.	- La variación de las condiciones o características de los enlaces intra-dominio, ocasionan inconvenientes de actualización en las tablas de rutas que manejan los equipos BGP. - Es posible que se generen bucles de enrutamiento, ocasionados por cambios en los valores IGP, para los cuales los equipos deben calcular nuevamente los costos de ruta causando largos periodos de convergencia en el sistema y pérdida transitoria de datos. - Los cambios de ruta afectan el normal funcionamiento de atributos como Local_Preference, MED u otros mecanismos que se basen en las características de las rutas, debido a que existirán equipos que recalculen la información de las rutas más rápido que otros.
Método de Sanción y Eliminación de Rutas: se compone por dos procesos, el primero consiste en aplicar sanciones a rutas que varían en periodos cortos de tiempo, consecuencia de la inestabilidad de las mismas, y el segundo proceso que elimina de las tablas, rutas que son inestables durante un largo periodo de tiempo evitando que se compartan rutas erróneas entre equipos de frontera; es realizado en tiempo real y dinámicamente, su monitoreo se realiza por medio de un Agente Monitor (MA: Monitor Agent) agregado al protocolo de enrutamiento BGP, el cual se encarga de registrar los tiempos mínimos y máximos de cambio en las rutas [38].	- Estos procesos mantienen actualizados más rápidamente las tablas de enrutamiento de los equipos de frontera, y sus vecinos. - El mecanismo retrasa el envío de los mensajes UPDATE, con el fin de enviarlos de manera consecutiva en un solo lote de estos mismos, evitando congestión en la red por el envío de mensajes UPDATE. - Proporciona una información en tiempo real y dinámica del estado de las rutas y sus variaciones.	- El proceso de sanción de rutas en tiempos cortos, ocasiona que el mensaje UPDATE sea enviado más frecuentemente generando un incremento de tráfico innecesario. - El tiempo de convergencia para que las rutas sean compartidas o eliminadas de las tablas de enrutamiento, puede ser un factor que perjudique el normal funcionamiento del mecanismo, ya que los equipos deben actualizar con mayor frecuencia sus tablas.

2.4 CONSIDERACIONES PARA MEJORAR LA TOMA DE DECISIONES DE ENRUTAMIENTO EN BGP-4 TENIENDO EN CUENTA TE

A pesar de que existen mecanismos que agregan capacidades de TE al proceso de enrutamiento en busca de seleccionar la "mejor ruta", es de gran importancia conocer las implicaciones que traen las adaptaciones del protocolo BGP-4, ya que estas podrían tener un efecto contrario al esperado y afectar el desempeño propio de la red. La manipulación de uno o más atributos propios del protocolo es un trabajo bastante complejo que necesita ser evaluado en primera instancia, en un simulador de redes antes de ser implementado en una red real, para evitar exponerse a no cumplir con las expectativas del administrador de red o a degradar el desempeño de la misma.

Considerando los mecanismos actuales que implementan capacidades de TE con el protocolo BGP-4, se podría tomar como referencia algunas de sus características que permitan realizar una adaptación eficiente al protocolo BGP-4, para mejorar la toma de decisiones de enrutamiento en busca de reducir la congestión entre diferentes AS. Las características más significativas son:

- ✓ **Uso del atributo LOCAL_PREFERENCE**: Se utiliza para controlar el tráfico saliente de un AS, minimizando la utilización de recursos de red y balanceando la carga de tráfico en los diferentes puntos de salida. Se considera el valor más alto de LOCAL_PREFERENCE como primer criterio según el proceso de decisión descrito en el ítem 1.2.3.

- ✓ **Uso del Atributo MED**: Controla el tráfico entrante de un AS, tomando como referencia el análisis de parámetros propios de una red. A pesar de no tener en cuenta las opiniones de los AS vecinos, el objetivo es determinar el enlace que presente menor métrica, debido a que ofrece las mejores condiciones para el tráfico.

- ✓ **Tiempo de Convergencia entre los Cambios de Ruta**: El tiempo de convergencia en una red debe ser mínimo para garantizar que no se presenten bucles de enrutamiento, que podrían entorpecer el funcionamiento de la red y afectar el desempeño de la misma.

Lo anterior indica que las soluciones que permiten agregar capacidades de TE al proceso de enrutamiento mediante el uso de atributos propios del protocolo BGP son bastante complejas, sin embargo se podrían realizar teniendo en cuenta tanto el control de tráfico entrante como el control de tráfico saliente.

2.5 SOLUCIÓN PROPUESTA PARA LA REDUCCIÓN DE LA CONGESTIÓN EN REDES IP MEDIANTE ADAPTACIÓN DEL PROTOCOLO BGP-4

La congestión en una red de telecomunicaciones es un fenómeno intrínseco, que afecta directamente el desempeño de la red. Por esta razón, la congestión se considera un parámetro fundamental que incide en la QoS y que tiene como efecto la pérdida de información.

Una de las formas de combatir la congestión que se presenta en las redes de telecomunicaciones, consiste en agregar dispositivos de red para generar nuevas rutas, lo que ocasiona un elevado incremento en los costos de implementación y operación. Cabe aclarar que existen diferentes mecanismos y algoritmos independientes, tanto a nivel de red

como a nivel de transporte, que pueden ser implementados por separado para reducir la congestión presente en una red; en caso de ser implementada una adaptación de BGP-4, se podría combatir la congestión conjuntamente con los mecanismos desarrollados actualmente.

El incremento del tráfico de paquetes en las redes IP, lleva a pensar en la necesidad de implementar protocolos de enrutamiento óptimos, que permitan direccionar eficientemente la información hacia su destino. Los enrutadores BGP se encargan de actualizar sus tablas de enrutamiento considerando la información de las rutas que emplean los enrutadores vecinos, con el objetivo de alcanzar un destino especifico, tomando como premisa el menor valor de métrica utilizada, sin embargo, no siempre toman las mejores decisiones de enrutamiento, lo que puede ocasionar problemas en la recepción de datos, ya que se generan retardos y en el peor de los casos pérdida de información. Este tipo de fallas se presentan principalmente porque el protocolo BGP-4 no cuenta con capacidades TE, que le permitan censar los enlaces con el fin de detectar si hay congestión que afecte el desempeño de la red.

La realización del proyecto "**Adaptaciones del Protocolo BGP-4 para Reducir la Congestión en Redes IP",** permite mediante el análisis de los atributos de BGP-4, realizar adaptaciones al algoritmo para analizar la factibilidad de mejorar la toma de decisiones de enrutamiento, en busca de reducir la congestión presente entre AS en redes IP.

La propuesta tiene como objetivo reducir la congestión que se presenta en una red y puede catalogarse como una solución para el control de congestión, ya que involucra a toda una red; este fenómeno se combate en el momento que las adaptaciones al protocolo BGP-4 consideran o basan su decisión en el algoritmo de enrutamiento, el cual toma como primer criterio la menor congestión presente en una ruta, permitiendo así que el camino antes seleccionado, procese los datos que tienen represados, evitando así contribuir a su saturación.

Como ya se mencionó en el inicio de este capítulo, pensar en la optimización de BGP-4 conlleva al análisis de la congestión en conjunto con los atributos propios del protocolo y sus métricas de enrutamiento [4].

En el capitulo anterior, se mencionaron causas que pueden generar el fenómeno de congestión, el cual afecta en forma directa el desempeño de la red. Por otro lado, se enumeran dos tipos de solución que se pueden tener en cuenta a la hora de afrontar este gran problema; la de bucle abierto, es la que previene la congestión en el dimensionamiento y posterior diseño de la red y la de bucle cerrado, que se aplica en este caso, por tratarse de una solución que actúa en el momento en que se presenta la falla, mediante la monitorización de parámetros como la pérdida de paquetes en una ruta, variable que va directamente relacionada con la congestión, así pues, a menor pérdida de paquetes, menor congestión en la ruta, y una posterior acción, representada en selección de la ruta que presente una menor congestión.

La congestión es un fenómeno que se puede cuantificar a través de la pérdida de paquetes, este último sirve como indicador, debido a que cuantifica la tasa de paquetes perdidos en una trasmisión de información, expresada en porcentajes. Así mismo la pérdida de paquetes se define como el complemento de los paquetes totales recibidos.

Entre las causas más comunes que originan la congestión en una red IP se encuentran los denominados factores intrínsecos como el deterioro del medio de comunicación, retardos presentes en el enlace, jitter, latencia, reducción del ancho de banda, además de la capacidad de procesamiento en los buffers de entrada y salida de los enrutadores de frontera. Es de anotar que TCP, permite retransmitir un paquete cuando este se haya perdido, lo que implica que al presentarse un alto nivel de retrasmisiones se genere una congestión de ruta y por tanto se pierda información.

El Protocolo de Mensajes de Control de Internet (ICMP: Internet Control Message Protocol), es un protocolo que opera a nivel de red y se utiliza para enviar mensajes de error desde un origen hacia un destino para verificar si un servicio, un host o un enrutador están o no disponibles en una red. En un caso real también se usa para cuantificar la tasa de pérdida de paquetes mediante el envío de mensajes con un número finito de paquetes y se contabiliza la cantidad que se reciben en la interfaz del destino. La expresión matemática para el cálculo de la tasa de pérdida de paquetes, donde nP_p es la tasa de paquetes perdidos, P_e el número de paquetes enviados en la transmisión y P_p es el número de paquetes perdidos en la misma, es [39]:

$$nP_p(\%) = \frac{P_p}{P_e}\ x\ 100\% \quad (1)$$

Evidentemente, el principal objetivo en el proceso de enrutamiento es encaminar la información por la ruta menos congestionada, evitando pérdidas de información que afecten el desempeño de la red. Garantizado que la ruta seleccionada por el dispositivo de enrutamiento es la que menos congestión presente a lo largo de su enlaces, se puede afirmar que el protocolo de enrutamiento posee capacidades de TE que puede aumentar el desempeño de la red.

Según lo anterior, en busca de reducir la congestión a nivel inter-dominio, la solución planteada para mejorar la toma de decisiones de enrutamiento, se basa en la aplicación de una política de selección de la mejor ruta considerando la menos congestionada, para lo cual se hace uso de la expresión matemática (1) definida en la resolución de CONATEL 2006, que permite determinar la tasa de pérdida de paquetes de información [39].

La adaptación al proceso de enrutamiento de BGP-4 que de ahora en adelante se conocerá como Protocolo de Pasarela de Frontera para Combatir la Congestión (BGP-C2: Border Gateway Protocol to Combate Congestion), al igual que el protocolo BGP-4 recibe y actualiza sus tablas, aplica políticas al tráfico entrante y saliente por medio de sus atributos.

BGP-C2, modifica el algoritmo de decisión de BGP-4, considerando el valor aleatorio de probabilidad de congestión en cada enlace, para calcular la congestión total presente en cada ruta, lo que implica que al camino con menor congestión le será asignado un menor costo como valor de métrica, valor que determinará la interfaz de salida mediante la asignación directa de un alto grado de preferencia por medio del atributo LOCAL_PREFERENCE. En el diagrama de la *Figura4,* se resume el procedimiento antes mencionado.

Para entender con más claridad la mecánica de selección de ruta basada en la congestión presente en cada enlace, se hace indispensable aclarar los términos convenidos en el diagrama de flujo, presentados en la Figura 4.

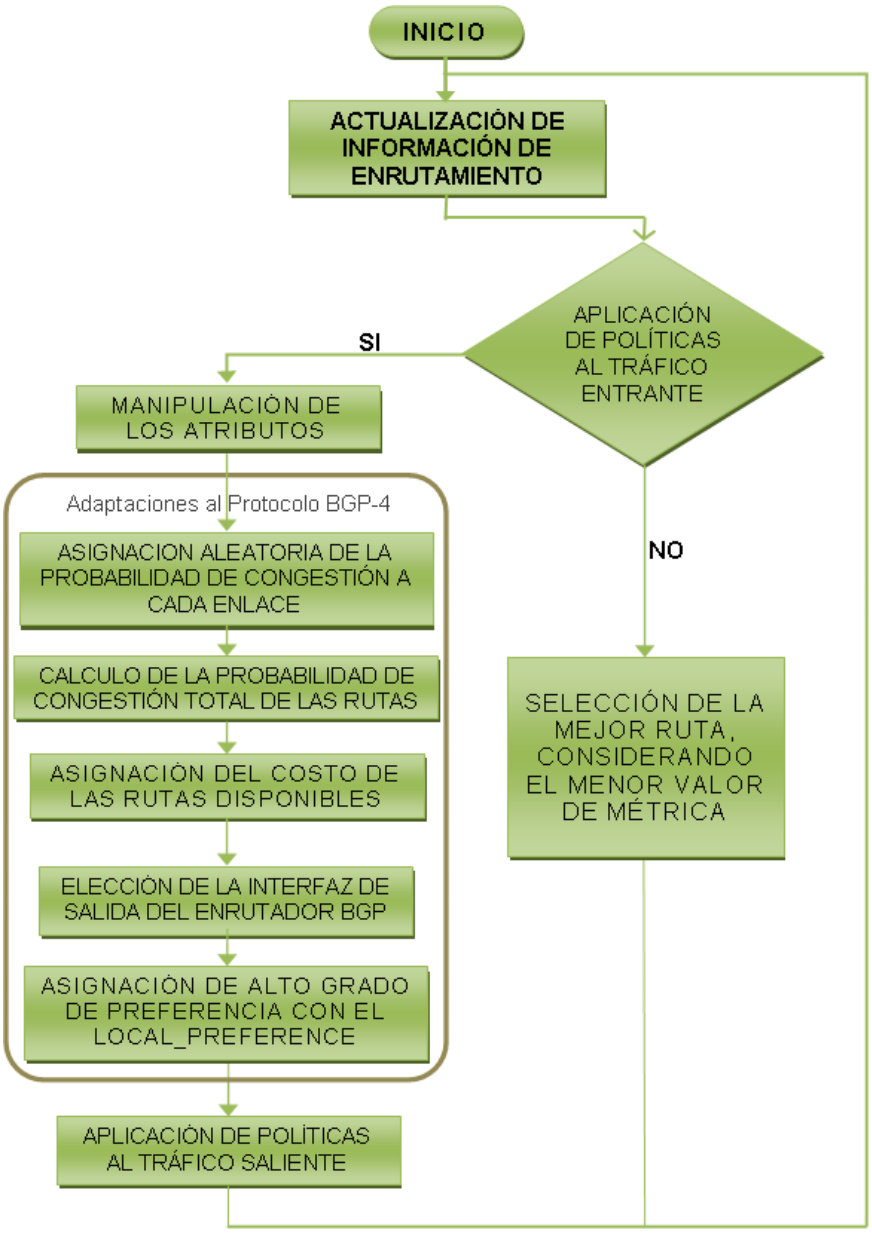

Figura 4 Proceso de Enrutamiento de BGP Modificado

2.5.1 Congestión de Ruta

La teoría de la probabilidad adopta el criterio de independencia estadística de eventos, el cual manifiesta que estos no están correlacionados entre sí, es decir, que la ocurrencia de un evento no afecta la probabilidad de ocurrencia de otro, de tal forma que, dos eventos A y B no vacios, se llaman independientes si ocurre que la probabilidad de A dado B es igual a la probabilidad de A (P(A|B)=P(A)) o que la probabilidad de B dado A es igual a la probabilidad de B (P(B|A)=P(B)), como conclusión, A y B son independientes si y sólo si $P(A \cap B) = P(A)P(B)$ [40].

En el análisis de la congestión en redes de telecomunicaciones, se aplica el criterio de independencia estadística de eventos el cual define que la probabilidad de congestión de un

enlace, no depende de la probabilidad de congestión de cualquier otro enlace que conforme la ruta [40].

La solución planteada exige considerar como eventos las siguientes variables para su análisis matemático:

- C_T: Congestión Total de la Ruta.
- E: Transferencia Exitosa.
- Di: Enlace i Disponible.
- Ci: Enlace i No Disponible.

Los eventos mencionados representan los diferentes casos que se pueden presentar durante la comunicación entre un equipo y otro, considerando la existencia de dos o más nodos que conforman una determinada ruta. Cada uno de los eventos se encuentra representado matemáticamente por una probabilidad que permite establecer a nivel inter-dominio, si el envío de datos entre un equipo trasmisor y otro receptor, será exitoso o no.

La C_T se considera como un evento probabilístico al cual se asocia una Probabilidad de Congestión Total de Ruta ($P(C_T)$), que considera las probabilidades de congestión presentes en cada enlace; sus valores oscilan entre 0 y 1, determinando el grado de bloqueo según el número de paquetes recibidos (P_R) respecto a los paquetes enviados (P_T).

$P(C_T)=0$ indica que cero paquetes de información se han perdido y $P(C_T)=1$ representa que ninguno de los paquetes de información enviados llegó al destino. Para el análisis de lo antes mencionado se debe tener en cuenta inicialmente, los valores de probabilidad ideales para dichos eventos, como se muestra a continuación: [40]:

- $P(C_T) = 0$
- $P(E) = 1$
- $P(Di) = 1$
- $P(Ci) = 0$

Para dar una solución optima al problema de congestión mediante una adaptación del Protocolo BGP-4, se debe calcular la $P(C_T)$, lo que permitirá determinar la mejor ruta considerando el menor valor de congestión total. Para tal fin, se presenta el siguiente análisis matemático. Por propiedad de complementos, lo anterior se puede relacionar así:

$$P(E) = 1 - P(C_T) \quad (2)$$

$$P(D_i) = 1 - P(C_i) \quad (3)$$

El evento E se presenta, si y sólo si, todos los enlaces que conforman la ruta se encuentran disponibles, como se muestra en la siguiente condición:

$$E = D_1 \cap D_2 \cap D_3 \cap D_4 \cap \dots\dots\dots\dots \cap D_n \quad (4)$$

Donde n, se entiende como el n-esimo enlace que conforma la ruta.

Ahora, la probabilidad de que el evento E ocurra, se expresa por la siguiente ecuación:

$$P(E) = P(D_1 \cap D_2 \cap D_3 \cap D_4 \cap \ldots\ldots\ldots\ldots \cap D_n) \quad (5)$$

Otra forma de expresar la anterior ecuación, es:

$$P(E) = P\left(\cap_{i=1}^{N} Di\right) \quad (6)$$

Esto se considera como la intersección de N eventos estadísticamente independientes, lo cual permite expresarlo como el producto de N términos, así:

$$P(E) = \prod_{i=1}^{N} P(Di) \quad (7)$$

Expandiéndose de esta manera:

$$P(E) = P(D_1) \times P(D_2) \times P(D_3) \times P(D_4) \times \ldots\ldots\ldots \times P(D_N) \quad (8)$$

Ahora, reemplazando en (8), las ecuaciones (2) y (3), se tiene que,

$$(1 - P(C_T)) = \left(1 - P(C_1)\right) \times \left(1 - P(C_2)\right) \times \left(1 - P(C_3)\right) \times \ldots\ldots\ldots\ldots \times (1 - P(C_N)) \quad (9)$$

Despejando,

$$P(C_T) = 1 - \left[\left(1 - P(C_1)\right) \times \left(1 - P(C_2)\right) \times \left(1 - P(C_3)\right) \times \ldots\ldots\ldots\ldots \times (1 - P(C_N))\right] \quad (10)$$

Otra forma de expresar la ecuación (11) es:

$$P(C_T) = 1 - \prod_{i=1}^{N}(1 - P(C_i)) \quad (11)$$

2.5.2 Pérdida de Paquetes de Información

Para el cálculo de la pérdida total de paquetes de información (P_P) en un ruta o los paquetes que no llegan al destino, se deben considerar los P_T y la $P(C_T)$. La formula (1) puede ser expresada en términos que han sido definidos anteriormente, así [39]:

$$P_p = P(C_T) \times P_T \quad (12)$$

2.5.3 Pérdida de Bytes de Información

Para calcular la pérdida total de bytes de información (B_P: Bytes Perdidos), en un ruta o los bytes que no llegan al destino, se deben considerar los Bytes Transmitidos (B_T: Bytes Transmitidos) y la $P(C_T)$ relacionados en la siguiente ecuación .

$$B_p = P(C_T) \times B_T \quad (13)$$

2.5.4 Costo de la Ruta

Como ya se mencionó anteriormente, el costo es una métrica de enrutamiento que es asignada arbitrariamente a cada enlace por el administrador de red; para el caso propuesto en este proyecto, el costo de la ruta corresponde a la magnitud de la $P(C_T)$. Por lo anterior se deduce

que la mejor ruta para el envío de datos es la que presente menor costo, debido a que los enlaces presentan una menor probabilidad de congestión, lo que implica menor número de bytes de información perdidos, optimizando así la selección de la mejor ruta.

2.5.5 El Atributo LOCAL_PREFERENCE

Inmediatamente después de considerar el menor valor de probabilidad de congestión y el costo total de la ruta, el protocolo BGP determina automáticamente el grado de preferencia de una ruta, teniendo como referencia el valor más bajo del costo anteriormente mencionado. Dicho grado de preferencia se expresa mediante el atributo LOCAL_PREFERENCE, el cual se asigna a un único punto de salida del AS sin importar la cantidad de rutas posibles a un destino en particular.

En síntesis, la solución planteada brinda al Protocolo BGP-4 capacidades de TE que le permiten determinar la mejor ruta para el envío de información, tomando como prioridad la ruta de menor congestión y por ende, la menor pérdida de información posible en el trayecto desde un origen a un destino especifico. Para tal efecto, en una topología de red planteada se han considerado variables de entrada y salida a los dominios involucrados. El uso del atributo LOCAL_PREFERENCE en conjunto con el monitoreo de los enlaces para determinar el grado de congestión, proporcionan al Protocolo BGP-4 una solución con características de TE para mejorar el proceso en la toma de decisiones de enrutamiento.

Según lo mencionado en el presente capítulo, se concluye que por medio de la adaptación del protocolo BGP-4 se podría optimizar el proceso de enrutamiento inter-dominio, considerando que existen diversas formas para lograrlo; cada una de ellas considera al menos un parámetro de red, una métrica de enrutamiento y un atributo propio del protocolo. El desarrollo de este proyecto propone una solución que mejora la toma de decisiones de enrutamiento basándose en la congestión presente en una ruta, la pérdida de información a lo largo de la misma, el costo como métrica de enrutamiento y el LOCAL_PREFERENCE, como atributo encargado de dar preferencia a la interfaz de salida del enrutador.

La investigación y el desarrollo de esta sección del documento, permiten la identificación del atributo, la métrica y el indicador a partir de los cuales se genera la propuesta de adaptación para mejorar la toma de decisiones de enrutamiento considerando la congestión en redes IP, en conjunto con el estudio matemático del cálculo de congestión presente en una ruta.

CAPITULO III: SIMULACIONES, PRUEBAS Y RESULTADOS

En el capítulo de simulaciones, pruebas y resultados, se muestran los escenarios de red utilizados para observar el comportamiento del protocolo BGP-4 en su versión estándar con respecto al protocolo BGP-4 adaptado, que de ahora en adelante se conocerá como BGP-C2, que busca reducir la congestión en redes IP mediante el mejoramiento en la toma de decisiones de enrutamiento. Las topologías de red utilizadas para simular el comportamiento de los protocolos en mención, se toman de la tesis de grado "*Estudio de Viabilidad para la Optimización de Enrutamiento IP con el Protocolo BGP*".

Los escenarios de simulación no necesariamente corresponden a topologías de red reales existentes actualmente en Internet; sin embargo, cumplen satisfactoriamente con diferentes características de red, que permiten comprobar la adaptación del protocolo BGP-C2, como se observan en la Tabla 3.

Tabla 3 Condiciones de Red

CONDICIONES	ESCENARIOS			
	1	2	3	4
Con más de una ruta	✓	✓	✓	✓
Con igual número de saltos inter-dominio			✓	✓
Con saltos intra-dominio en un dominio		✓	✓	✓
Con más de dos dominios	✓	✓		
Con empate entre rutas inter e intra-dominio				✓
Con dominios intermedios entre cliente y servidor	✓	✓		

Por otro lado, en un ambiente de red real, el protocolo de enrutamiento BGP estándar, tanto a nivel intra-dominio como inter-dominio, intercambia exclusivamente información de enrutamiento entre los dispositivos de red, lo que implica, que la información relacionada con los parámetros de red a lo largo de una ruta no se comparte, salvo que sea entre dominios adyacentes. Pese a lo anterior, en el entorno de simulación en el que se desarrolla el proyecto, el algoritmo es capaz de conocer la congestión total presente en una determinada ruta a partir de las congestiones de cada enlace; con el fin de verificar el correcto funcionamiento del algoritmo de BGP-C2 en cuanto a la selección de una ruta, son asignados valores aleatorios de congestión para cada una de las rutas involucradas; además, se debe resaltar que el entorno de simulación toma un enlace como un salto de un AS a otro, sin contar el sistema autónomo origen, y el valor del costo que es asignado por defecto por SSFNet, es uno por enlace.

Ahora bien en un entorno real, gracias al atributo Communities que permite segmentar la red reuniendo un grupo de rutas con características similares, es posible obtener datos acerca del comportamiento de una misma Comunidad.

El análisis de resultados, tiene como base la información obtenida en las tablas de enrutamiento de los enrutadores de frontera de cada escenario propuesto, mediante la herramienta de simulación SSFnet, utilizada para el desarrollo del proyecto (ver Anexo A). Es de anotar, que los resultados obtenidos a lo largo de la simulación y los códigos DML creados para verificar la solución, se presentan en el Anexo A.

Por otro lado, el protocolo BGP-C2 permite asignar un valor de LOCAL_PREFERENCE más alto al enlace origen de la ruta que presentó menor congestión y por ende una menor pérdida

de información; los valores de congestión presentes en cada uno de los enlaces que conforman una ruta, pueden ser aleatorios, similar a como se pueden presentar en una red real y en este capítulo se analiza la respuesta de BGP-C2 a dichos cambios. Sin embargo, los cambios en los valores de congestión ocurren en periodos de tiempo diferentes, lo cual indica que el grado de bloqueo se mantendrá durante todo el tiempo de simulación.

Por último hay que resaltar, que en cada escenario de simulación se configuró un cliente HTTP para que envíe paquetes aleatorios de tamaño constante durante veinte mil segundos (20.000 segundos), lo anterior permite mostrar que la congestión afecta el desempeño de la red considerando la información recibida respecto a la enviada. Es por esto que los paquetes enviados en cada ejecución son de tamaño constante, para evitar una interpretación equivoca del efecto de la congestión, por estar directamente relacionado el tamaño de los paquetes, el tiempo en que el simulador procesa la información y el tiempo de simulación total.

3.1 ESCENARIOS DE SIMULACIÓN

3.1.1 Escenario de Simulación No1

El primer modelo de red propuesto consta de cinco dominios, cada uno con su respectivo enrutador de frontera, como se muestra en la *Figura5*. El tráfico de la información se realiza entre el AS1, dominio donde se encuentra ubicado un cliente HTTP y el AS2, dominio donde está presente el servidor HTTP; se observa que la mayoría de los dominios se encuentran conectados entre sí, a excepción del AS2 con el AS4 y el AS1 con el AS3. Existen diferentes rutas para enviar información del AS1 al AS2. Las posibles rutas se mencionan a continuación [10]:

- ✓ **Ruta 1:** Conexión directa entre los AS1 y AS2. Presenta un solo enlace.
- ✓ **Ruta 2:** Conexión indirecta entre los AS1 y AS2 a través del AS5. Presenta dos enlaces.
- ✓ **Ruta 3:** Conexión indirecta entre los AS1 y AS2 a través de los AS4 y AS3. Presenta tres enlaces.
- ✓ **Ruta 4:** Conexión indirecta entre los AS1 y AS2 a través de los AS4 y AS5. Presenta tres enlaces.
- ✓ **Ruta 5:** Conexión indirecta entre los AS1 y AS2 a través de los AS4, AS3 y AS5. Presenta cuatro enlaces.
- ✓ **Ruta 6:** Conexión indirecta entre los AS1 y AS2 a través de los AS5, AS4 y AS3. Presenta cuatro enlaces.
- ✓ **Ruta 7:** Conexión indirecta entre los AS1 y AS2 a través de los AS5 y AS3. Presenta tres enlaces.

En el escenario de la *Figura5*, únicamente se muestran tres rutas posibles para enviar información desde un cliente HTTP hasta un servidor HTTP, ya que se consideran suficientes para comprobar el buen funcionamiento del algoritmo modificado BGP-C2. Es de esperar que el protocolo BGP-4, para el tráfico de información seleccione la ruta 1, considerando que es la que atraviesa el menor número de sistemas autónomos, independiente de la congestión presente en la ruta. Para el mismo escenario; la propuesta de BGP-C2 es seleccionar la ruta que presente una menor congestión total.

El objetivo de incorporar un cliente y un servidor HTTP radica en que los resultados obtenidos muestran el número de paquetes al igual que el número de bytes enviados y recibidos, lo que implica demostrar que BGP-C2 optimiza la toma de decisiones de enrutamiento, considerando la congestión como parámetro de red. El funcionamiento esperado de BGP-C2 es la selección de la ruta de menor pérdida de paquetes implicando la disminución de la congestión en la red, mediante la selección de la ruta más adecuada.

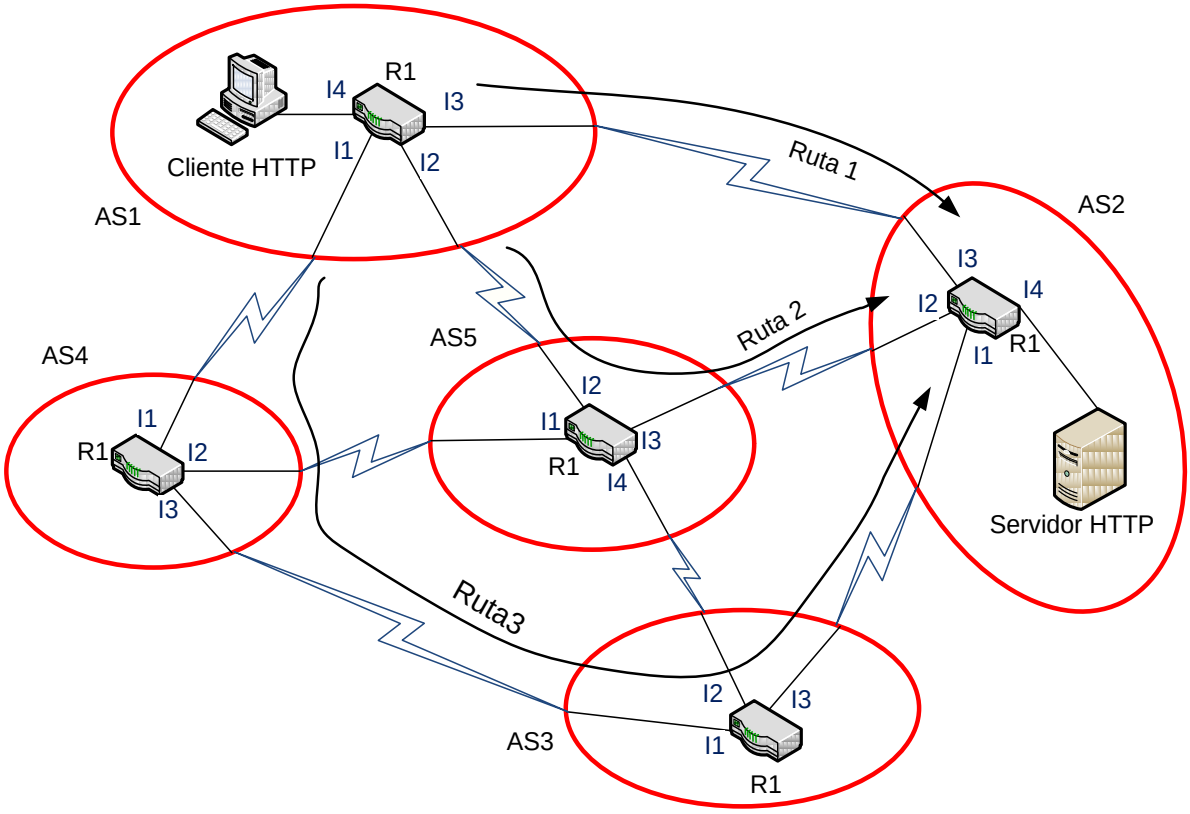

Figura 5 Escenario de Simulación1

3.1.2 Escenario de Simulación No2

El segundo escenario de red se representa por tres AS conectados entre sí. Los datos se envían desde un cliente HTTP ubicado en el AS1 y el servidor HTTP situado en el AS2. El sistema autónomo 3 posee dos enrutadores de frontera, esto con el objetivo de probar que BGP-C2 puede aprovechar las propiedades de direccionamiento intra-dominio.

Como se muestra en la *Figura 6*, las dos posibles rutas para enviar información desde el AS1 al AS2 son:

- ✓ **Ruta 1:** Conexión directa entre los AS1 y AS2. Presenta un solo enlace.
- ✓ **Ruta 2:** Conexión indirecta entre los AS1 y AS2 a través del AS3. Presenta dos enlaces. Dos enlaces inter-dominio y salto intra-dominio.

El protocolo BGP-4 según su algoritmo de decisión, selecciona la ruta 1 para el envío de información, considerando que es la que atraviesa el menor número de sistemas autónomos en comparación a la ruta 2. BGP-C2 basa su decisión en la congestión total de ruta presente.

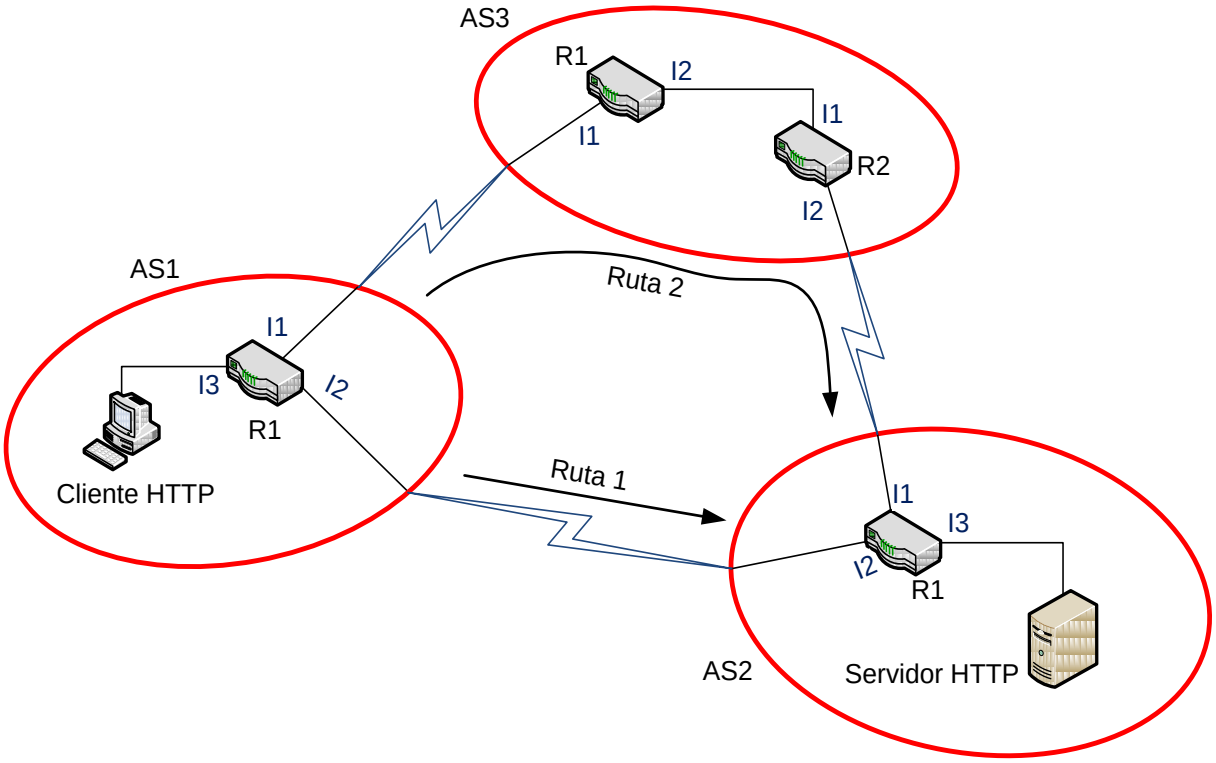

Figura 6 Escenario de Simulación 2

3.1.3 Escenario de Simulación No3

Este escenario de simulación está representado por el AS1 y el AS2 conectados entre sí. La principal característica de esta topología de red es que cada uno de los dominios implicados cuenta con 2 enrutadores de frontera denominados R1 y R2. La información se envía desde un cliente HTTP ubicado en un punto específico del AS1 a un servidor HTTP conectado al R2 del AS2. A continuación se muestra un posible escenario de red el cual posee un cliente HTTP conectado a R2 en el AS1.

El escenario de red que se muestra en la *Figura 7*, cuenta con dos posibles rutas para el tráfico de información entre el cliente y el servidor HTTP:

a. Ruta 1: Conexión directa entre los dominios AS1y AS2. La comunicación se realiza entre los enrutadores de frontera R2 de los sistemas autónomos presentes. Presenta un solo enlace.

b. Ruta 2: Conexión directa entre los dominios AS1 y AS2. La información sale del enrutador de frontera R2 del AS1 y pasa por el enrutador R1 de su mismo dominio. Su siguiente salto es el enrutador R1 del AS2, dispositiva que se conecta a su vez con R2 del dominio AS2. Presenta dos saltos intra-dominio y un enlace inter-dominio.

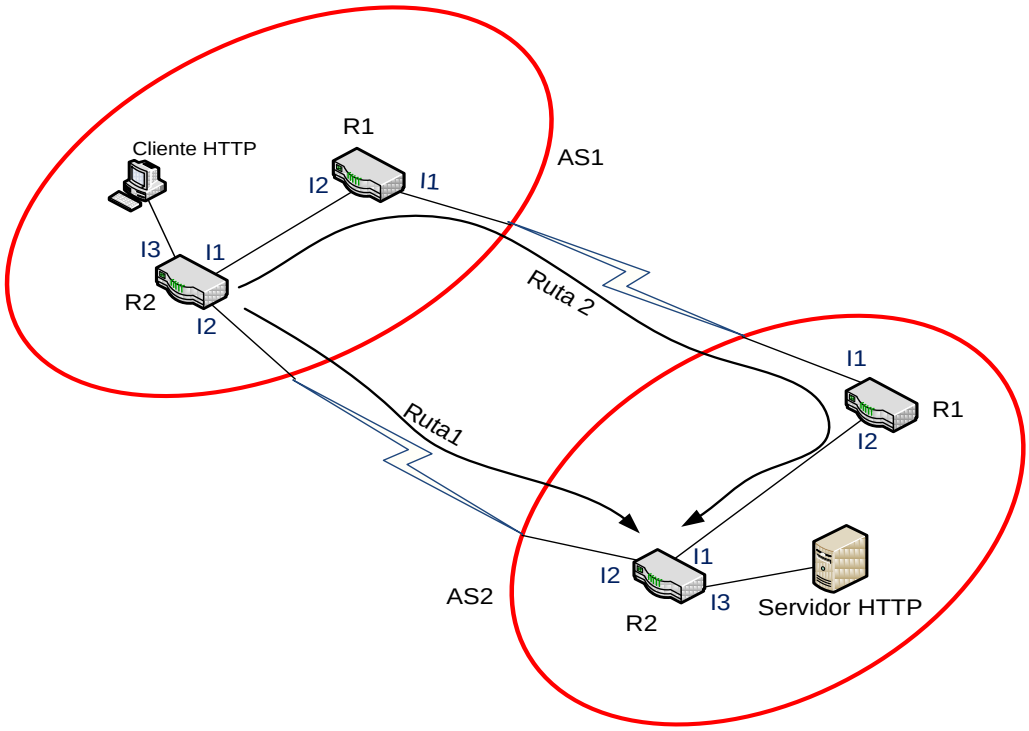

Figura 7 Escenario de Simulación 3

La decisión de enrutamiento que toma el algoritmo BGP-4 para el envío de información, considera el menor número de enlaces; para este escenario de red, la ruta 1 es la que presenta menor cantidad de enlaces. El algoritmo BGP-C2, optimiza esa decisión y toma como ruta la que menor congestión total presente a lo largo de la ruta.

3.1.4 Escenario de Simulación No4

El modelo de red que se muestra en la *Figura 8*, posee conectado un cliente HTTP al R1 del AS1 e indica dos posibles rutas para el envío de información entre el origen y el destino:

a. **Ruta 1:** Conexión directa entre los dominios AS1 y AS2. El punto de salida del AS1 es R1, pasando por el enrutador de frontera R1 del AS2. Dicho enrutador se conecta al R2 de su mismo AS, dicho dispositivo vinculado al servidor HTTP. Presenta un salto intra-dominio y un enlace inter-dominio.

b. **Ruta 2:** Conexión directa entre los dominios AS1 y AS2. El punto de salida del AS1 es R1; la información pasa por R2 presente en el mismo dominio. El punto de llegada es R2 del AS2. Presenta un salto intra-dominio y un enlace inter-dominio.

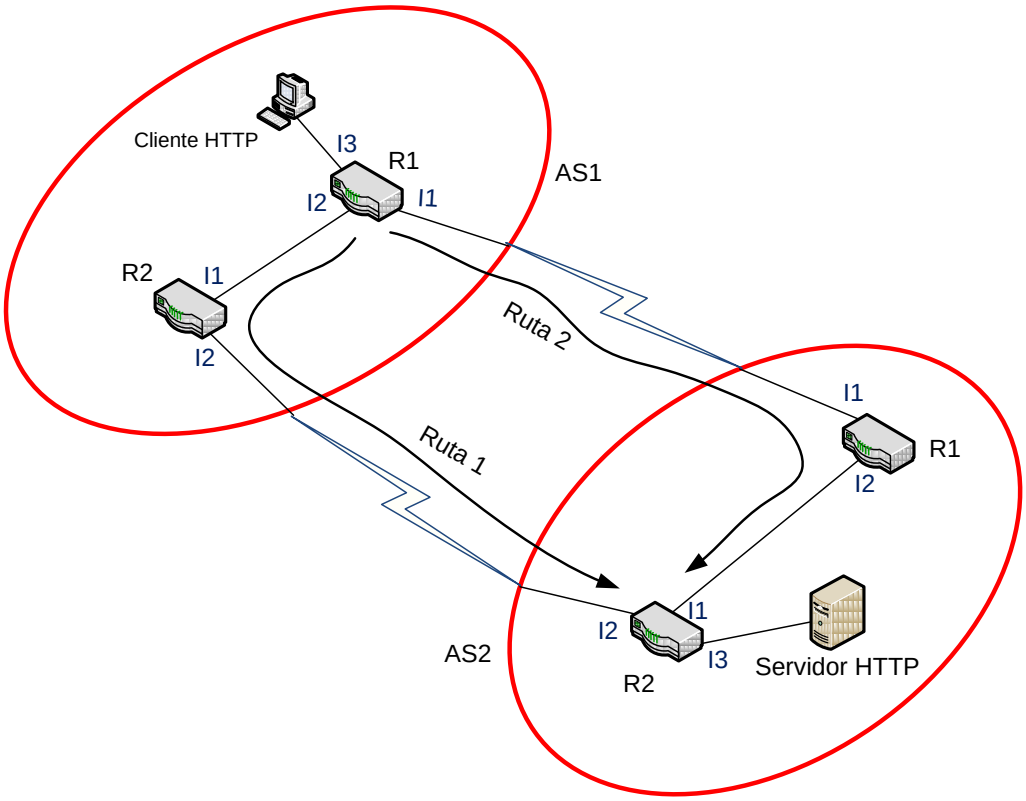

Figura 8 Escenario de Simulación 4

Para este modelo de red se espera que el protocolo BGP-4, al igual que los anteriores escenarios, tome como criterio de decisión el menor número de enlaces entre origen y destino.

Como se puede observar en la figura 8, las rutas 1 y 2 poseen el mismo número de enlaces, considerando tanto los saltos intra-dominio como los inter-dominio; a este suceso se le conoce como empate entre rutas, por lo que el algoritmo de decisión de BGP-4, debe aplicar criterios de desempate para determinar la mejor ruta. Estos criterios son los que se exponen en la sección 1.2.3 del Capítulo I.

3.2 SIMULACIONES

Para cada uno de los escenarios, se ejecutan los protocolo BGP-4 y BGP-C2; en el primer caso, la tabla de enrutamiento que arrojará el simulador, indicará que la ruta seleccionada por el algoritmo de decisión será siempre la que menor número de sistemas autónomos atraviese, por las características propias del protocolo, independiente de los valores de congestión que puedan presentarse; en el segundo caso, el protocolo considerará diferentes valores de congestión en distintos instantes de tiempo (t1, t2, …., tn), lo cual permitirá visualizar, por medio de las tablas de enrutamiento, las diferentes rutas tomadas por el algoritmo de decisión del protocolo BGP-C2 y poder mostrar el buen funcionamiento del mismo.

Los resultados obtenidos a través de las simulaciones realizadas en este capítulo corresponden a las topologías de red propuestas en el ítem 3.1, considerando los algoritmos de decisión de BGP-4 y BGP-C2.

El análisis de los resultados, tendrá en cuenta las tablas de enrutamiento que se obtienen de los dispositivos que intervienen en el proceso de comunicación originado por el simulador; dichas tablas contienen información relevante para el análisis de enrutamiento (ver Anexo A). Por otro lado, para establecer unos valores de pérdida de paquetes máximos y mínimos, se considera el algoritmo de BGP-4 con y sin congestión. Además se incluyen graficas que permiten cuantificar el efecto de la congestión en una red IP para los algoritmos BGP-4 y BGP-C2, cuya interpretación se encuentra en el Anexo A.

3.2.1 Escenario1

3.2.1.1 Escenario1: BGP-4

La *Figura 9*, muestra que la ruta1 es la seleccionada por el enrutador de frontera R1 del AS1 para enviar la información; la cual utiliza un salto para llegar al R1 del AS2. BGP-4 basa su decisión en el criterio del menor número de saltos presentes a lo largo de la ruta. Ahora bien la congestión presente en las rutas es 0, lo que implica que toda la información enviada es entregada al receptor. La totalidad de paquetes enviados es de 61 y corresponde a 8.822.973 bytes como se muestra en la *Figura 10*.

```
.....................................................................
.........................   bgp@1:1 wrap-up   .........................
.....................................................................
~# 1:1   --- Loc-RIB at bgp@1:1:
~# 1:1  |      NetworkNHI         NextHopNHI       Metric LocPrf Weight ASPathNHI
~# 1:1  | *>   2                   2:1(3)                -      -      - 2
~# 1:1  | *>   3                   2:1(3)                -      -      - 2 3
~# 1:1  | *>   4                   4:1(1)                -      -      - 4
~# 1:1  | *>   1                   self                  -      -      -           i
~# 1:1  | *>   5                   5:1(2)                -      -      - 5

.....................................................................
```

Figura 9 Tabla de Enrutamiento de R1 presente en el AS1. BGP-4. Escenario1.

Para mostrar el efecto de la congestión en una red IP, al Escenario1, se asigna una congestión total de ruta aleatoria, para generar una pérdida de paquetes durante la transmisión. Ahora bien, en la *Figura 11*, se muestra el efecto que produce la congestión, aclarando que la decisión del algoritmo de BGP-4 no considera el grado de bloqueo de las tres posibles rutas, por lo que tomara por defecto la más corta como se observa en la figura 9.

```
93.663275782 [ sid 0 start 60.416673721 ] clnt 1:2 srv 2:2(0) #pages: 2 #objects: 2 total: 11083B seconds: 33.246602061 SUCCESS
103.383367213 [ sid 1 start 103.374386921 ] clnt 1:2 srv 2:2(0) #pages: 1 #objects: 1 total: 3229B seconds: 0.006980292 SUCCESS
288.001042913 [ sid 2 start 110.667457871 ] clnt 1:2 srv 2:2(0) #pages: 2 #objects: 3 total: 332547B seconds: 177.333585042 SUCCESS
376.623090644 [ sid 3 start 330.098051406 ] clnt 1:2 srv 2:2(0) #pages: 2 #objects: 7 total: 34901B seconds: 46.525039238 SUCCESS
397.646332867 [ sid 4 start 397.632125381 ] clnt 1:2 srv 2:2(0) #pages: 1 #objects: 1 total: 9138B seconds: 0.014207486 SUCCESS
674.394859193 [ sid 5 start 674.38203873 ] clnt 1:2 srv 2:2(0) #pages: 1 #objects: 1 total: 7360B seconds: 0.012820463 SUCCESS
1453.487522228 [ sid 6 start 762.415628847 ] clnt 1:2 srv 2:2(0) #pages: 16 #objects: 32 total: 137513B seconds: 691.071893381 SUCCESS
1746.60041013 [ sid 7 start 1502.708661089 ] clnt 1:2 srv 2:2(0) #pages: 7 #objects: 9 total: 42462B seconds: 243.891749041 SUCCESS
3150.481346518 [ sid 8 start 1781.088111012 ] clnt 1:2 srv 2:2(0) #pages: 30 #objects: 67 total: 666388B seconds: 1369.393235506 SUCCESS
3177.97044006 [ sid 9 start 3177.961853445 ] clnt 1:2 srv 2:2(0) #pages: 1 #objects: 1 total: 2713B seconds: 0.008586615 SUCCESS
3246.361523251 [ sid 10 start 3214.893829949 ] clnt 1:2 srv 2:2(0) #pages: 2 #objects: 2 total: 4938B seconds: 31.467693302 SUCCESS
3307.515137934 [ sid 11 start 3306.857276023 ] clnt 1:2 srv 2:2(0) #pages: 1 #objects: 2 total: 8925B seconds: 0.657861911 SUCCESS
3822.628238058 [ sid 12 start 3464.442890671 ] clnt 1:2 srv 2:2(0) #pages: 9 #objects: 19 total: 295255B seconds: 358.185347387 SUCCESS
4355.856560838 [ sid 13 start 3837.053742418 ] clnt 1:2 srv 2:2(0) #pages: 3 #objects: 3 total: 15182B seconds: 518.80281842 SUCCESS
4972.74363615 [ sid 14 start 4357.074225299 ] clnt 1:2 srv 2:2(0) #pages: 9 #objects: 23 total: 185182B seconds: 615.669410851 SUCCESS
5041.906447585 [ sid 15 start 5006.547363956 ] clnt 1:2 srv 2:2(0) #pages: 2 #objects: 5 total: 26838B seconds: 35.359083629 SUCCESS
5830.235782099 [ sid 16 start 5677.400129295 ] clnt 1:2 srv 2:2(0) #pages: 5 #objects: 10 total: 36894B seconds: 152.835652804 SUCCESS
5967.374953582 [ sid 17 start 5848.366438284 ] clnt 1:2 srv 2:2(0) #pages: 4 #objects: 27 total: 145762B seconds: 119.008515298 SUCCESS
6480.331797369 [ sid 18 start 6025.765255773 ] clnt 1:2 srv 2:2(0) #pages: 8 #objects: 12 total: 206518B seconds: 454.566541596 SUCCESS
6638.447761895 [ sid 19 start 6511.919254535 ] clnt 1:2 srv 2:2(0) #pages: 4 #objects: 8 total: 95428B seconds: 126.52850736 SUCCESS
7190.992671277 [ sid 20 start 6679.231663545 ] clnt 1:2 srv 2:2(0) #pages: 9 #objects: 26 total: 395033B seconds: 511.761007732 SUCCESS
7470.819702181 [ sid 21 start 7467.412050265 ] clnt 1:2 srv 2:2(0) #pages: 1 #objects: 10 total: 88926B seconds: 3.407651916 SUCCESS
7830.385488129 [ sid 22 start 7695.151492399 ] clnt 1:2 srv 2:2(0) #pages: 4 #objects: 6 total: 23392B seconds: 135.23399573 SUCCESS
7914.467287249 [ sid 23 start 7914.458963085 ] clnt 1:2 srv 2:2(0) #pages: 1 #objects: 1 total: 2369B seconds: 0.008324164 SUCCESS
8062.788742266 [ sid 24 start 8062.779882519 ] clnt 1:2 srv 2:2(0) #pages: 1 #objects: 1 total: 3071B seconds: 0.008859747 SUCCESS
8199.063396881 [ sid 25 start 8159.705712991 ] clnt 1:2 srv 2:2(0) #pages: 2 #objects: 10 total: 83791B seconds: 39.35768389 SUCCESS
9060.236970369 [ sid 26 start 8449.147014752 ] clnt 1:2 srv 2:2(0) #pages: 16 #objects: 31 total: 185034B seconds: 611.089955617 SUCCESS
9330.140944931 [ sid 27 start 9108.090632425 ] clnt 1:2 srv 2:2(0) #pages: 6 #objects: 6 total: 28005B seconds: 222.050312506 SUCCESS
9879.173610105 [ sid 28 start 9383.070439633 ] clnt 1:2 srv 2:2(0) #pages: 12 #objects: 19 total: 133798B seconds: 496.103170472 SUCCESS
11016.061387351 [ sid 29 start 9979.046041837 ] clnt 1:2 srv 2:2(0) #pages: 23 #objects: 39 total: 787096B seconds: 1037.015345514 SUCCESS
11164.203984554 [ sid 30 start 11048.87367433 ] clnt 1:2 srv 2:2(0) #pages: 3 #objects: 8 total: 57958B seconds: 115.330310224 SUCCESS
11318.534319001 [ sid 31 start 11179.181732937 ] clnt 1:2 srv 2:2(0) #pages: 5 #objects: 5 total: 85804B seconds: 139.352586064 SUCCESS
11542.294097374 [ sid 32 start 11344.948112157 ] clnt 1:2 srv 2:2(0) #pages: 6 #objects: 11 total: 32526B seconds: 197.345985217 SUCCESS
11982.865334323 [ sid 33 start 11552.976731277 ] clnt 1:2 srv 2:2(0) #pages: 12 #objects: 22 total: 187363B seconds: 429.888603046 SUCCESS
12438.734396449 [ sid 34 start 12006.608150622 ] clnt 1:2 srv 2:2(0) #pages: 10 #objects: 30 total: 221354B seconds: 432.126245827 SUCCESS
12612.48211922 [ sid 35 start 12609.315929316 ] clnt 1:2 srv 2:2(0) #pages: 1 #objects: 10 total: 49254B seconds: 3.166189904 SUCCESS
12852.700941886 [ sid 36 start 12710.979931821 ] clnt 1:2 srv 2:2(0) #pages: 5 #objects: 9 total: 78373B seconds: 141.721010065 SUCCESS
13051.57572927 [ sid 37 start 12886.927253588 ] clnt 1:2 srv 2:2(0) #pages: 5 #objects: 47 total: 275582B seconds: 164.648475682 SUCCESS
13198.933050524 [ sid 38 start 13198.111437414 ] clnt 1:2 srv 2:2(0) #pages: 1 #objects: 2 total: 20651B seconds: 0.82161311 SUCCESS
13199.680959409 [ sid 39 start 13199.671814322 ] clnt 1:2 srv 2:2(0) #pages: 1 #objects: 1 total: 3445B seconds: 0.009145087 SUCCESS
13291.459762896 [ sid 40 start 13249.77630798 ] clnt 1:2 srv 2:2(0) #pages: 2 #objects: 4 total: 30841B seconds: 41.683454916 SUCCESS
13341.71071122 [ sid 41 start 13341.701871309 ] clnt 1:2 srv 2:2(0) #pages: 1 #objects: 1 total: 3045B seconds: 0.008839911 SUCCESS
13381.795166675 [ sid 42 start 13378.395964359 ] clnt 1:2 srv 2:2(0) #pages: 1 #objects: 5 total: 60854B seconds: 3.399202316 SUCCESS
13401.430521102 [ sid 43 start 13401.224992689 ] clnt 1:2 srv 2:2(0) #pages: 1 #objects: 2 total: 5292B seconds: 0.205528331 SUCCESS
14236.150936101 [ sid 44 start 13498.307648849 ] clnt 1:2 srv 2:2(0) #pages: 15 #objects: 106 total: 2134392B seconds: 737.843287252 SUCCESS
14489.568341609 [ sid 45 start 14329.571609161 ] clnt 1:2 srv 2:2(0) #pages: 6 #objects: 11 total: 204909B seconds: 159.996732448 SUCCESS
14970.713036538 [ sid 46 start 14667.152141396 ] clnt 1:2 srv 2:2(0) #pages: 10 #objects: 22 total: 394361B seconds: 303.560895142 SUCCESS
15193.704427969 [ sid 47 start 15192.271991539 ] clnt 1:2 srv 2:2(0) #pages: 1 #objects: 7 total: 39661B seconds: 1.43243643 SUCCESS
15928.56064198 [ sid 48 start 15266.957047202 ] clnt 1:2 srv 2:2(0) #pages: 11 #objects: 13 total: 696208 seconds: 661.603594778 SUCCESS
16350.171161178 [ sid 49 start 16062.96789228 ] clnt 1:2 srv 2:2(0) #pages: 10 #objects: 15 total: 88251B seconds: 287.203268898 SUCCESS
16815.728576294 [ sid 50 start 16649.205585164 ] clnt 1:2 srv 2:2(0) #pages: 5 #objects: 11 total: 73667B seconds: 166.52299113 SUCCESS
16936.739852088 [ sid 51 start 16936.541612343 ] clnt 1:2 srv 2:2(0) #pages: 1 #objects: 2 total: 6889B seconds: 0.198239745 SUCCESS
17036.022382984 [ sid 52 start 17031.204378902 ] clnt 1:2 srv 2:2(0) #pages: 1 #objects: 13 total: 96062B seconds: 4.818004082 SUCCESS
17082.70475858 [ sid 53 start 17082.479597628 ] clnt 1:2 srv 2:2(0) #pages: 1 #objects: 2 total: 4938B seconds: 0.225160952 SUCCESS
17586.606139613 [ sid 54 start 17117.550651924 ] clnt 1:2 srv 2:2(0) #pages: 10 #objects: 36 total: 229670B seconds: 469.057487689 SUCCESS
17588.353685083 [ sid 55 start 17587.791848262 ] clnt 1:2 srv 2:2(0) #pages: 1 #objects: 3 total: 21543B seconds: 0.561836821 SUCCESS
18923.246561134 [ sid 56 start 17614.348159895 ] clnt 1:2 srv 2:2(0) #pages: 21 #objects: 32 total: 214176B seconds: 1308.898401445 SUCCESS
19264.278533663 [ sid 57 start 18958.125319864 ] clnt 1:2 srv 2:2(0) #pages: 7 #objects: 9 total: 74123B seconds: 306.153213799 SUCCESS
19462.38869611 [ sid 58 start 19321.242524586 ] clnt 1:2 srv 2:2(0) #pages: 6 #objects: 9 total: 59898B seconds: 141.146171524 SUCCESS
19483.066070624 [ sid 59 start 19483.057062104 ] clnt 1:2 srv 2:2(0) #pages: 1 #objects: 1 total: 3266B seconds: 0.00900852 SUCCESS
19908.433173769 [ sid 60 start 19594.649106356 ] clnt 1:2 srv 2:2(0) #pages: 8 #objects: 12 total: 76468B seconds: 313.784067413 SUCCESS
-----------------------------------------------------------------------
| 1 timelines, 5 barriers, 344552 events, 2063 ms, 172 Kevt/s
-----------------------------------------------------------------------
```

Figura 10 Paquetes recibidos en el Servidor HTTP sin Congestión. BGP-4 Escenario 1

```
579.260652741 [ sid 0 start 60.416673721 ] clnt 1:2 srv 2:2(0) #pages: 2 #objects: 2 total: 11083B seconds: 518.84397902 SUCCESS
771.080144172 [ sid 1 start 588.97176388 ] clnt 1:2 srv 2:2(0) #pages: 1 #objects: 1 total: 3229B seconds: 182.108380292 SUCCESS
2776.531910124 [ sid 2 start 778.36423483 ] clnt 1:2 srv 2:2(0) #pages: 2 #objects: 3 total: 332547B seconds: 1998.167675294 SUCCESS
4382.648503755 [ sid 3 start 2818.628918617 ] clnt 1:2 srv 2:2(0) #pages: 2 #objects: 7 total: 34901B seconds: 1564.019585138 SUCCESS
4646.470945978 [ sid 4 start 4403.657538492 ] clnt 1:2 srv 2:2(0) #pages: 1 #objects: 1 total: 9138B seconds: 242.813407486 SUCCESS
5166.018672304 [ sid 5 start 4923.206651841 ] clnt 1:2 srv 2:2(0) #pages: 1 #objects: 1 total: 7360B seconds: 242.812020463 SUCCESS
12622.087367112 [ sid 6 start 5254.039441958 ] clnt 1:2 srv 2:2(0) #pages: 16 #objects: 32 total: 137513B seconds: 7368.047925154 SUCCESS
14796.893124097 [ sid 7 start 12671.308505973 ] clnt 1:2 srv 2:2(0) #pages: 7 #objects: 9 total: 42462B seconds: 2125.584618124 SUCCESS
-----------------------------------------------------------------------
| 1 timelines, 5 barriers, 332978 events, 1563 ms, 221 Kevt/s
-----------------------------------------------------------------------
```

Figura 11 Paquetes recibidos en el Servidor HTTP con Congestión. BGP-4 Escenario 1

3.2.1.2 Escenario1: BGP-C2 en t1

La *Figura 12*, muestra la tabla de enrutamiento del R1 del AS1, en la que se observa que la ruta seleccionada por el algoritmo de BGP-C2 es la misma, con la excepción de que esta vez, toma como criterio de decisión la menor congestión presente entre las posibles rutas (ver *Tabla 4*). Para determinar la interfaz de salida para el envío de información se asigna un alto valor de LOCAL_PREFERENCE (100), el cual está relacionado directamente con bajo costo de ruta, métrica que corresponde a un bajo grado de congestión y por tanto a una baja tasa de pérdida de información.

```
.....................................................................
.........................   bgp@1:1 wrap-up   .........................
.....................................................................
~# 1:1   --- Loc-RIB at bgp@1:1:
~# 1:1  |      NetworkNHI          NextHopNHI       Metric LocPrf Weight ASPathNHI
~# 1:1  | *>   2                    2:1(3)              -    100      - 2
~# 1:1  | *>   3                    2:1(3)              -    100      - 2 3
~# 1:1  | *>   4                    2:1(3)              -    100      - 2 3 4
~# 1:1  | *>   1                    self                -      -      -              i
~# 1:1  | *>   5                    2:1(3)              -    100      - 2 5

.....................................................................
```

Figura 12 Tabla de Enrutamiento R1 presente en el AS1. Protocolo BGP-C2 en t1. Escenario 1.

Tabla 4 Congestión presente en cada Ruta. Escenario 1 BGP-C2 en t1

Ruta	Congestión	P. Perdidos	B. Perdidos
Ruta1	0.29	18	3.488.091
Ruta2	0.49	30	5.610.238
Ruta3	0.78	48	7.816.809

3.2.1.2.1 Gráfica de Paquetes y Bytes Perdidos vs Tasa de Pérdidas.

La *Figura 13* y la *Figura 14*, muestran los paquetes y los bytes perdidos respectivamente, para diferentes valores de congestión, recordando que esta es la ruta seleccionada por el algoritmo de decisión de BGP-C2. La cantidad de paquetes de información que se envía es igual a la que se envía en el BGP-4, lo anterior para determinar cuál de los dos protocolos de enrutamiento en mención escoge la ruta con menor congestión. Se puede notar que la ruta a pesar de ser la misma que la seleccionada por el protocolo BGP-4 está menos congestionada y por lo tanto puede enviar más paquetes durante el mismo tiempo de simulación.

Tabla 5 Paquetes Perdidos y Tasa de Pérdida en la Ruta 1. Escenario 1 BGP-C2

Escenario1_BGP-C2		
P. Recibidos	**P. Perdidos**	**Tasa de Pérdida**
60	0	0.%
59	1	1.67%
57	3	5%
54	6	10%
47	13	21.67%
44	16	26.67%
29	31	51.67%

La *Figura 13*, representa gráficamente los datos consignados en la *Tabla 5*.

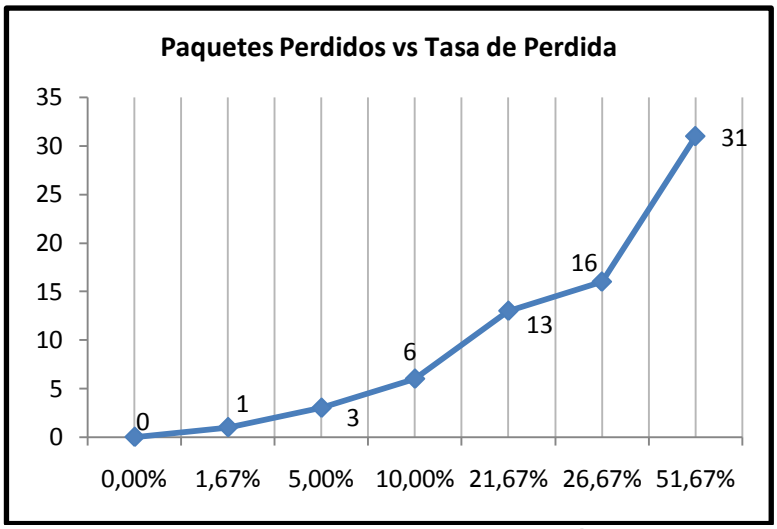

Figura 13 Paquetes Perdidos vs. Tasa de Pérdida. BGP-C2

Tabla 6 Bytes Perdidos y Tasa de Pérdida en la Ruta1. Escenario 1 BGP-C2

Escenario1_BGP-C2		
B. Recibidos	**B. Perdidos**	**Tasa de Pérdida**
8,746,505	0	0%
8,743,239	3,266	0.04%
8,609,218	137,287	1.57%
8,143,829	602,676	6.89%
7,764,741	981,764	11.22%
5,031,079	3,715,426	42.48%
3,131,641	5,614,864	64.20%

La *Figura 14*, representa gráficamente los datos consignados en la *Tabla 6*.

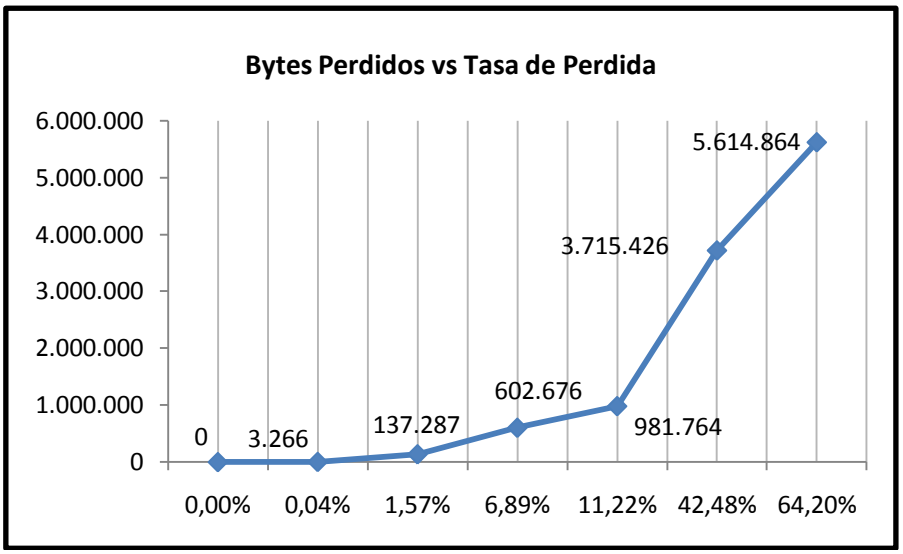

Figura 14 Bytes Perdidos vs. Tasa de Pérdidas. BGP-C2

3.2.1.3 Escenario1: BGP-C2 en t2

La *Figura 15*, muestra las tablas de enrutamiento del R1 del AS1 y del AS5, en las que se observa que para enviar la información desde el R1 del AS1 hacia el R1 del AS2, la ruta seleccionada por el algoritmo de BGP-C2 es la ruta2, lo que indica que la información pasa a través del AS5 para llegar a su destino. La primera tabla de enrutamiento indica que los paquetes que pasan por el AS5 van directamente al R1 del AS2. La segunda tabla y la más importante para el caso de estudio, muestra que la ruta seleccionada por el algoritmo de BGP-C2 a pesar de no ser la ruta con el mayor número de saltos, es la menos congestionada (ver *Tabla 7*). Ahora, para definir la interfaz de salida del enrutador se asigna un valor de 100 al atributo LOCAL_PREFERENCE, el cual está relacionado inversamente con el costo, inversamente con la probabilidad de congestión y a la pérdida de paquetes de información

```
.....................................................................
.........................   bgp@5:1 wrap-up   .........................
.....................................................................
~# 5:1   --- Loc-RIB at bgp@5:1:
~# 5:1  |      NetworkNHI         NextHopNHI       Metric LocPrf Weight ASPathNHI
~# 5:1  | *>   2                   2:1(2)                -      -      - 2
~# 5:1  | *>   3                   3:1(2)                -      -      - 3
~# 5:1  | *>   4                   4:1(2)                -      -      - 4
~# 5:1  | *>   1                   1:1(2)                -      -      - 1
~# 5:1  | *>   5                   self                  -      -      -           i

.....................................................................
.........................   bgp@1:1 wrap-up   .........................
.....................................................................
~# 1:1   --- Loc-RIB at bgp@1:1:
~# 1:1  |      NetworkNHI         NextHopNHI       Metric LocPrf Weight ASPathNHI
~# 1:1  | *>   2                   5:1(2)                -    100      - 5 2
~# 1:1  | *>   3                   5:1(2)                -    100      - 5 3
~# 1:1  | *>   4                   5:1(2)                -    100      - 5 4
~# 1:1  | *>   1                   self                  -      -      -           i
~# 1:1  | *>   5                   5:1(2)                -    100      - 5

.....................................................................
```

Figura 15 Tabla de Enrutamiento R1 presente en el AS1 Protocolo BGP-C2 en t2 Escenario 1.

Tabla 7 Congestión presente en cada Ruta. Escenario1 BGP-C2 en t2

Ruta	Congestión	P. Perdidos	B. Perdidos
Ruta1	0.18	12	3.363.963
Ruta2	0.05	3	256.151
Ruta3	0.39	24	4.332.593

3.2.1.3.1 Graficas de Paquetes y Bytes Perdidos vs Tasa de Pérdidas.

La *Tabla 8* y *Tabla 9*, muestra la cantidad de paquetes y bytes perdidos para diversos valores de congestión (ver *Figura 16* y *Figura 17*), haciendo claridad que la ruta 2 es la ruta seleccionada por el algoritmo de decisión de BGP-C2. Como se había mencionado en apartes anteriores, el tamaño de los paquetes de información es aleatorio pero se mantiene constante tanto para ejecuciones del protocolo BGP-4 como para las de BGP-C2, lo anterior para determinar cuál de los dos protocolos de enrutamiento en mención escoge la ruta con menor congestión. Se puede notar que la ruta a pesar de ser más larga que la seleccionada por el

protocolo BGP-4 está menos congestionada y por lo tanto puede enviar más paquetes durante el mismo tiempo de simulación; claro está que el paquete que le precede, alcance a ser enviado en el tiempo de simulación restante.

Tabla 8 Paquetes Perdidos y Tasa de Pérdida en la Ruta2. Escenario1 BGP-C2

Escenario1_BGP-C2		
P. Recibidos	**P. Perdidos**	**Tasa de Pérdida**
60	0	0%
58	2	3.33%
57	3	5%
56	4	6.67%
48	12	20%
44	16	26.67%
29	31	51.67%

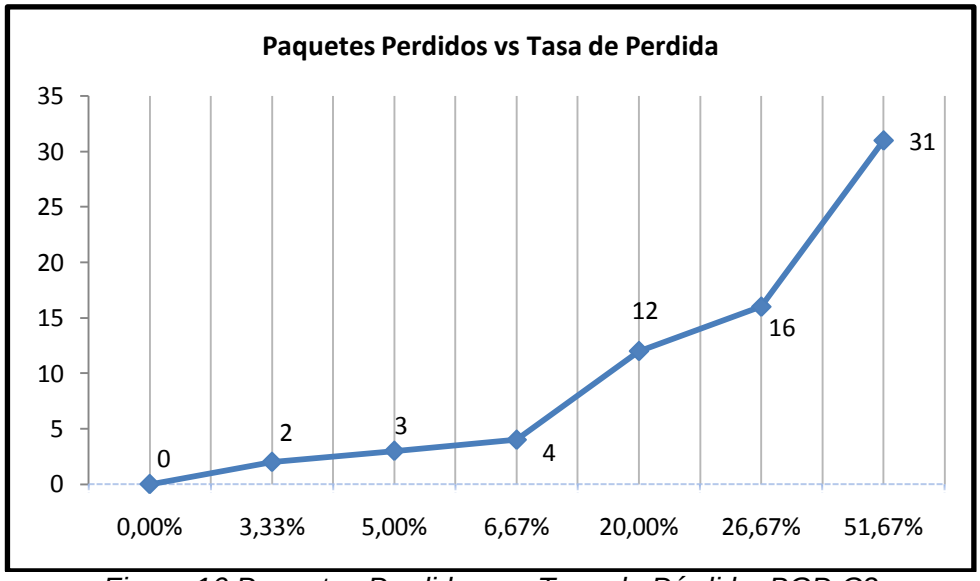

Figura 16 Paquetes Perdidos vs. Tasa de Pérdida. BGP-C2

Tabla 9 Bytes Perdidos y Tasa de Pérdida en la Ruta2. Escenario1 BGP-C2

Escenario1_BGP-C2		
B. Recibidos	**B. Perdidos**	**Tasa de Pérdida**
8,746,505	0	0
8,683,341	63,164	0.72%
8,609,218	137,287	1.57%
8,395,042	351,463	4.02%
7,804,402	942,103	10.77%
5,031,079	3,715,426	42.48%
3,131,641	5,614,864	64.20%

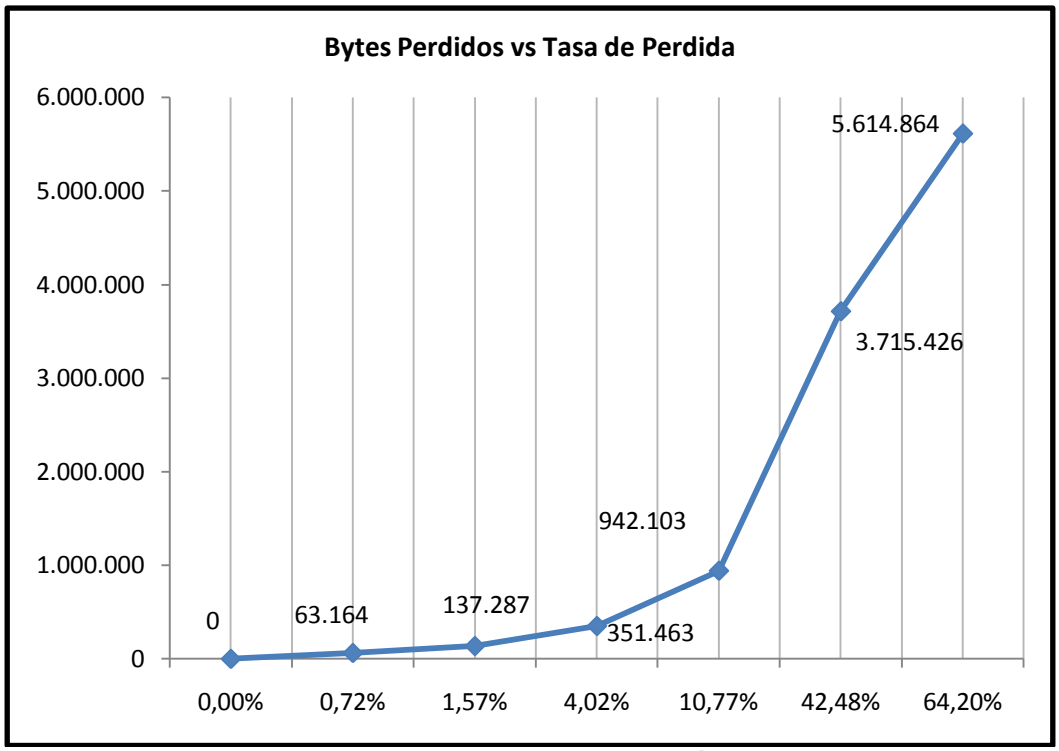

Figura 17 Bytes Perdidos vs. Tasa de Pérdida.BGP-C2

3.2.1.4 Escenario1: BGP-C2 en t3

La *Figura18*, muestra las tablas de enrutamiento del R1 del AS1, del AS3 y el AS4, en las que se observa que para enviar la información desde el R1 del AS1 hacia el R1 del AS2, la ruta seleccionada por el algoritmo de BGP-C2 es la ruta3, lo que indica que la información pasa a través de los AS3 y AS4 para llegar a su destino. La primera tabla de enrutamiento indica que los paquetes pasan por el AS4, luego por el AS3 y finalmente llegan a su destino. La siguiente es la tabla de enrutamiento del R1 del AS4, la cual indica que la información va a pasar a través del AS3 para alcanzar finalmente el destino. Ahora la última tabla de enrutamiento, nos dice que para enviar la información al R1 del AS2, hace un solo salto. Esto indica que a pesar de ser la ruta más larga de las tres posibles, BGP-C2 selecciona la que menor congestión tenga, por medio de su algoritmo de decisión (ver *Tabla 10*). Inmediatamente después, a la interfaz de salida se asigna un valor alto de LOCAL_PREFERENCE, éste asociado directamente a un bajo costo de ruta e inversamente a la congestión y a la pérdida de paquetes.

```
.....................................................................
.........................   bgp@1:1 wrap-up   .........................
.....................................................................
~# 1:1   --- Loc-RIB at bgp@1:1:
~# 1:1  |      NetworkNHI         NextHopNHI       Metric LocPrf Weight ASPathNHI
~# 1:1  | *>   2                   4:1(1)                -    100      - 4 3 2
~# 1:1  | *>   3                   4:1(1)                -    100      - 4 3
~# 1:1  | *>   4                   4:1(1)                -    100      - 4
~# 1:1  | *>   1                   self                  -      -      -            i
~# 1:1  | *>   5                   4:1(1)                -    100      - 4 5

.....................................................................
.........................   bgp@4:1 wrap-up   .........................
.....................................................................
~# 4:1   --- Loc-RIB at bgp@4:1:
~# 4:1  |      NetworkNHI         NextHopNHI       Metric LocPrf Weight ASPathNHI
~# 4:1  | *>   2                   3:1(1)                -      -      - 3 2
~# 4:1  | *>   3                   3:1(1)                -      -      - 3
~# 4:1  | *>   4                   self                  -      -      -            i
~# 4:1  | *>   1                   1:1(1)                -      -      - 1
~# 4:1  | *>   5                   5:1(1)                -      -      - 5

.....................................................................
.........................   bgp@3:1 wrap-up   .........................
.....................................................................
~# 3:1   --- Loc-RIB at bgp@3:1:
~# 3:1  |      NetworkNHI         NextHopNHI       Metric LocPrf Weight ASPathNHI
~# 3:1  | *>   2                   2:1(1)                -      -      - 2
~# 3:1  | *>   3                   self                  -      -      -            i
~# 3:1  | *>   4                   4:1(3)                -      -      - 4
~# 3:1  | *>   1                   2:1(1)                -      -      - 2 1
~# 3:1  | *>   5                   5:1(4)                -      -      - 5

.....................................................................
```

Figura 18 Tabla de Enrutamiento R1 presente en el AS1. Protocolo BGP-C2 en t3 Escenario 1.

Tabla 10 Congestión presente en cada Ruta. Escenario 1 BGP-C2 en t3

Ruta	Congestión	P. Perdidos	B. Perdidos
Ruta1	0.29	18	3.488.091
Ruta2	0.26	16	3.463.995
Ruta3	0.05	3	256.151

3.2.1.4.1 Grafica de Paquetes y Bytes Perdidos vs Tasa de Pérdida.

La *Tabla 11 y Tabla 12*, al igual que los ejemplos anteriores muestra el número de paquetes y bytes perdidos obtenidos a través de varias ejecuciones con valores de congestión aleatorios, resaltando que la ruta3 es la seleccionada por el algoritmo de decisión de BGP-C2 (ver *Figura 19* y *Figura 20* respectivamente). Las características de transmisión son idénticas a los casos anteriores. Se puede observar que la ruta a pesar de tener mayor número de enlaces, presenta menos congestión que las otras dos posibles.

Tabla 11 Paquetes Perdidos y Tasa de Pérdida en la Ruta3. Escenario 1 BGP-C2.

Escenario1_BGP-C2		
P. Recibidos	**P. Perdidos**	**Tasa de Pérdidas**
60	0	0%
58	2	3.33%
57	3	5%
56	4	6.67%
48	12	20%
44	16	26.67%
29	31	51.67%

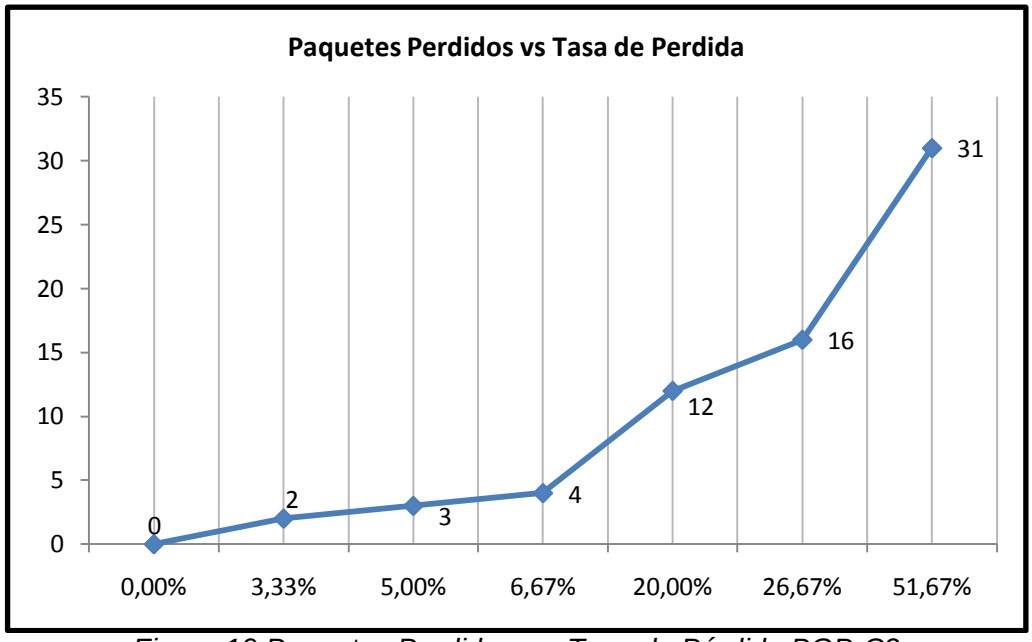

Figura 19 Paquetes Perdidos vs. Tasa de Pérdida.BGP-C2

Tabla 12 Bytes Perdidos y Tasa de Pérdida en la Ruta3. Escenario1 BGP-C2

Escenario1_BGP-C2		
B. Recibidos	**B. Perdidos**	**Tasa de Pérdida**
8,746,505	0	0%
8,683,341	63,164	0.72%
8,609,218	137,287	1.57%
8,395,042	351,463	4.02%
7,804,402	942,103	10.77%
5,031,079	3,715,426	42.48%
3,131,641	5,614,864	64.20%

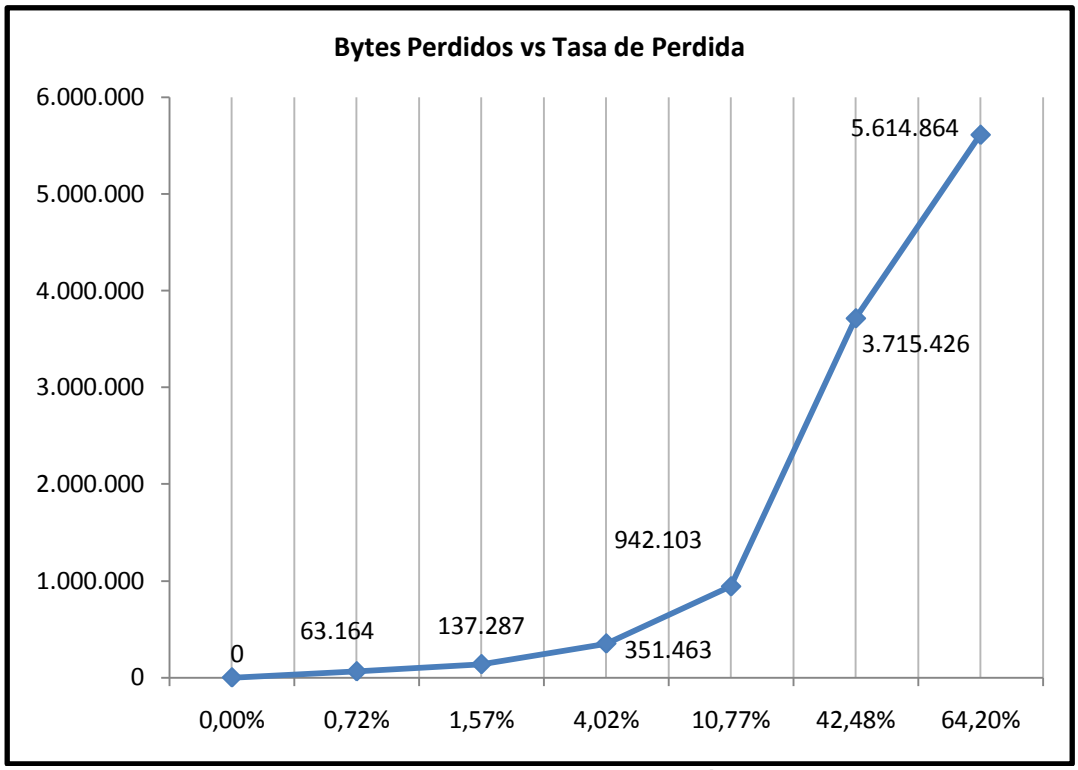

Figura 20 Bytes Perdidos vs. Tasa de Pérdida.BGP-C2

3.2.2 Escenario2

3.2.2.1 Escenario2: BGP-4

La tabla de enrutamiento de la *Figura 21*, indica que BGP-4 selecciona la ruta1 para enviar la información desde el cliente HTTP que se encuentra conectado al R1 del AS1, hasta el servidor conectado al R1 del AS2, dicha decisión se toma considerando el criterio del menor número de enlaces, presentes entre destino y origen. Como en la topología anterior, se ejecuta BGP-4 sin considerar congestión en los enlaces, lo que implica que la máxima información recibida es la que corresponde al mínimo índice de pérdida de paquetes, esto es de 61 paquetes, equivalentes a 8.822.973 como se muestra en la *Figura 22*.

```
.....................................................................
.........................   bgp@1:1 wrap-up   .........................
.....................................................................
~# 1:1   --- Loc-RIB at bgp@1:1:
~# 1:1  |      NetworkNHI         NextHopNHI       Metric LocPrf Weight ASPathNHI
~# 1:1  | *>   3                   3:1(1)                -      -      - 3
~# 1:1  | *>   2                   2:1(2)                -      -      - 2
~# 1:1  | *>   1                   self                  -      -      -           i

.....................................................................
```

Figura 21 Tabla de Enrutamiento R1 presente en el AS1. Protocolo BGP-4 Escenario 2

```
93.663275782 [ sid 0 start 60.416673721 ] clnt 1:2 srv 2:2(0) #pages: 2 #objects: 2 total: 11083B seconds: 33.246602061 SUCCESS
103.383367213 [ sid 1 start 103.374386921 ] clnt 1:2 srv 2:2(0) #pages: 1 #objects: 1 total: 3229B seconds: 0.008980292 SUCCESS
288.001042913 [ sid 2 start 110.667457871 ] clnt 1:2 srv 2:2(0) #pages: 2 #objects: 3 total: 332547B seconds: 177.333585042 SUCCESS
376.623090644 [ sid 3 start 330.098051406 ] clnt 1:2 srv 2:2(0) #pages: 2 #objects: 7 total: 34901B seconds: 46.525039238 SUCCESS
397.646332867 [ sid 4 start 397.632125381 ] clnt 1:2 srv 2:2(0) #pages: 1 #objects: 1 total: 9138B seconds: 0.014207486 SUCCESS
674.394859193 [ sid 5 start 674.38203873 ] clnt 1:2 srv 2:2(0) #pages: 1 #objects: 1 total: 7360B seconds: 0.012820463 SUCCESS
1453.487522228 [ sid 6 start 762.415628847 ] clnt 1:2 srv 2:2(0) #pages: 16 #objects: 32 total: 137513B seconds: 691.071893381 SUCCESS
1746.60041013 [ sid 7 start 1502.708661089 ] clnt 1:2 srv 2:2(0) #pages: 7 #objects: 9 total: 42462B seconds: 243.891749041 SUCCESS
3150.481334457 [ sid 8 start 1781.088111012 ] clnt 1:2 srv 2:2(0) #pages: 30 #objects: 67 total: 666388B seconds: 1369.393223445 SUCCESS
3177.970427999 [ sid 9 start 3177.961841384 ] clnt 1:2 srv 2:2(0) #pages: 1 #objects: 1 total: 2713B seconds: 0.008586615 SUCCESS
3246.36151119 [ sid 10 start 3214.893817888 ] clnt 1:2 srv 2:2(0) #pages: 2 #objects: 2 total: 4938B seconds: 31.467693302 SUCCESS
3307.515125873 [ sid 11 start 3306.857263962 ] clnt 1:2 srv 2:2(0) #pages: 1 #objects: 2 total: 8925B seconds: 0.657861911 SUCCESS
3822.628225997 [ sid 12 start 3464.44287861 ] clnt 1:2 srv 2:2(0) #pages: 9 #objects: 19 total: 295255B seconds: 358.185347387 SUCCESS
4355.856548777 [ sid 13 start 3837.053730357 ] clnt 1:2 srv 2:2(0) #pages: 3 #objects: 3 total: 15182B seconds: 518.80281842 SUCCESS
4972.743624089 [ sid 14 start 4357.074213238 ] clnt 1:2 srv 2:2(0) #pages: 9 #objects: 23 total: 185182B seconds: 615.669410851 SUCCESS
5041.906435524 [ sid 15 start 5006.547351895 ] clnt 1:2 srv 2:2(0) #pages: 2 #objects: 5 total: 26838B seconds: 35.359083629 SUCCESS
5830.235770038 [ sid 16 start 5677.400117234 ] clnt 1:2 srv 2:2(0) #pages: 5 #objects: 10 total: 36894B seconds: 152.835652804 SUCCESS
5967.374941521 [ sid 17 start 5848.366426223 ] clnt 1:2 srv 2:2(0) #pages: 4 #objects: 27 total: 145762B seconds: 119.008515298 SUCCESS
6480.331785308 [ sid 18 start 6025.765243712 ] clnt 1:2 srv 2:2(0) #pages: 8 #objects: 12 total: 206518B seconds: 454.566541596 SUCCESS
6638.447749834 [ sid 19 start 6511.919242474 ] clnt 1:2 srv 2:2(0) #pages: 4 #objects: 8 total: 95428B seconds: 126.52850736 SUCCESS
7190.992659216 [ sid 20 start 6679.231651484 ] clnt 1:2 srv 2:2(0) #pages: 9 #objects: 26 total: 395033B seconds: 511.761007732 SUCCESS
7470.81969012 [ sid 21 start 7467.412038204 ] clnt 1:2 srv 2:2(0) #pages: 1 #objects: 10 total: 88926B seconds: 3.407651916 SUCCESS
7830.385476068 [ sid 22 start 7695.151480338 ] clnt 1:2 srv 2:2(0) #pages: 4 #objects: 6 total: 23392B seconds: 135.23399573 SUCCESS
7914.467275188 [ sid 23 start 7914.458951024 ] clnt 1:2 srv 2:2(0) #pages: 1 #objects: 1 total: 2369B seconds: 0.008324164 SUCCESS
8062.788730205 [ sid 24 start 8062.779870458 ] clnt 1:2 srv 2:2(0) #pages: 1 #objects: 1 total: 3071B seconds: 0.008859747 SUCCESS
8199.06338482 [ sid 25 start 8159.70570093 ] clnt 1:2 srv 2:2(0) #pages: 2 #objects: 10 total: 83791B seconds: 39.35768389 SUCCESS
9060.236958308 [ sid 26 start 8449.147002691 ] clnt 1:2 srv 2:2(0) #pages: 16 #objects: 31 total: 185034B seconds: 611.089955617 SUCCESS
9330.14093287 [ sid 27 start 9108.090620364 ] clnt 1:2 srv 2:2(0) #pages: 6 #objects: 6 total: 28005B seconds: 222.050312506 SUCCESS
9879.173598044 [ sid 28 start 9383.070427572 ] clnt 1:2 srv 2:2(0) #pages: 12 #objects: 19 total: 133798B seconds: 496.103170472 SUCCESS
11016.06137529 [ sid 29 start 9979.046029776 ] clnt 1:2 srv 2:2(0) #pages: 23 #objects: 39 total: 787096B seconds: 1037.015345514 SUCCESS
11164.203972493 [ sid 30 start 11048.873662269 ] clnt 1:2 srv 2:2(0) #pages: 3 #objects: 8 total: 57958B seconds: 115.330310224 SUCCESS
11318.53430694 [ sid 31 start 11179.181720876 ] clnt 1:2 srv 2:2(0) #pages: 5 #objects: 5 total: 85804B seconds: 139.352586064 SUCCESS
11542.294085313 [ sid 32 start 11344.948100096 ] clnt 1:2 srv 2:2(0) #pages: 6 #objects: 11 total: 32526B seconds: 197.345985217 SUCCESS
11982.865322262 [ sid 33 start 11552.976719216 ] clnt 1:2 srv 2:2(0) #pages: 12 #objects: 22 total: 187363B seconds: 429.888603046 SUCCESS
12438.734384388 [ sid 34 start 12006.608138561 ] clnt 1:2 srv 2:2(0) #pages: 10 #objects: 30 total: 221354B seconds: 432.126245827 SUCCESS
12612.482107159 [ sid 35 start 12609.315917255 ] clnt 1:2 srv 2:2(0) #pages: 1 #objects: 10 total: 49254B seconds: 3.166189904 SUCCESS
12852.700929825 [ sid 36 start 12710.97991976 ] clnt 1:2 srv 2:2(0) #pages: 5 #objects: 9 total: 78373B seconds: 141.721010065 SUCCESS
13051.575717209 [ sid 37 start 12886.927241527 ] clnt 1:2 srv 2:2(0) #pages: 5 #objects: 47 total: 275582B seconds: 164.648475682 SUCCESS
13198.933038463 [ sid 38 start 13198.111425353 ] clnt 1:2 srv 2:2(0) #pages: 1 #objects: 2 total: 20651B seconds: 0.82161311 SUCCESS
13199.680947348 [ sid 39 start 13199.671802261 ] clnt 1:2 srv 2:2(0) #pages: 1 #objects: 1 total: 3445B seconds: 0.009145087 SUCCESS
13291.459750835 [ sid 40 start 13249.776295919 ] clnt 1:2 srv 2:2(0) #pages: 2 #objects: 4 total: 30841B seconds: 41.683454916 SUCCESS
13341.710699159 [ sid 41 start 13341.701859248 ] clnt 1:2 srv 2:2(0) #pages: 1 #objects: 1 total: 3045B seconds: 0.008839911 SUCCESS
13381.795154614 [ sid 42 start 13378.395952298 ] clnt 1:2 srv 2:2(0) #pages: 1 #objects: 5 total: 60854B seconds: 3.399202316 SUCCESS
13401.430508959 [ sid 43 start 13401.224980628 ] clnt 1:2 srv 2:2(0) #pages: 1 #objects: 2 total: 5292B seconds: 0.205528331 SUCCESS
14236.15092404 [ sid 44 start 13498.307636788 ] clnt 1:2 srv 2:2(0) #pages: 15 #objects: 106 total: 2134392B seconds: 737.843287252 SUCCESS
14489.568329548 [ sid 45 start 14329.5715971 ] clnt 1:2 srv 2:2(0) #pages: 6 #objects: 11 total: 204909B seconds: 159.996732448 SUCCESS
14970.713024477 [ sid 46 start 14667.152129335 ] clnt 1:2 srv 2:2(0) #pages: 10 #objects: 22 total: 394361B seconds: 303.560895142 SUCCESS
15193.704415908 [ sid 47 start 15192.271979478 ] clnt 1:2 srv 2:2(0) #pages: 1 #objects: 7 total: 39661B seconds: 1.43243643 SUCCESS
15928.560629919 [ sid 48 start 15266.957035141 ] clnt 1:2 srv 2:2(0) #pages: 11 #objects: 13 total: 69620B seconds: 661.603594778 SUCCESS
16350.171149117 [ sid 49 start 16062.967880219 ] clnt 1:2 srv 2:2(0) #pages: 10 #objects: 15 total: 88251B seconds: 287.203268898 SUCCESS
16815.728564233 [ sid 50 start 16649.205573103 ] clnt 1:2 srv 2:2(0) #pages: 5 #objects: 11 total: 73667B seconds: 166.52299113 SUCCESS
16936.739840027 [ sid 51 start 16936.541600282 ] clnt 1:2 srv 2:2(0) #pages: 1 #objects: 2 total: 6889B seconds: 0.198239745 SUCCESS
17036.022370923 [ sid 52 start 17031.204366841 ] clnt 1:2 srv 2:2(0) #pages: 1 #objects: 13 total: 96062B seconds: 4.818004082 SUCCESS
17082.704746519 [ sid 53 start 17062.479585567 ] clnt 1:2 srv 2:2(0) #pages: 1 #objects: 2 total: 4938B seconds: 0.225160952 SUCCESS
17586.608127552 [ sid 54 start 17117.550639863 ] clnt 1:2 srv 2:2(0) #pages: 10 #objects: 36 total: 229670B seconds: 469.057487689 SUCCESS
17588.353673022 [ sid 55 start 17587.791836201 ] clnt 1:2 srv 2:2(0) #pages: 1 #objects: 3 total: 21543B seconds: 0.561836821 SUCCESS
18923.246549279 [ sid 56 start 17614.348147834 ] clnt 1:2 srv 2:2(0) #pages: 21 #objects: 32 total: 214176B seconds: 1308.898401445 SUCCESS
19264.278521602 [ sid 57 start 18958.125307803 ] clnt 1:2 srv 2:2(0) #pages: 7 #objects: 9 total: 74123B seconds: 306.153213799 SUCCESS
19462.388684049 [ sid 58 start 19321.242512525 ] clnt 1:2 srv 2:2(0) #pages: 6 #objects: 9 total: 59898B seconds: 141.146171524 SUCCESS
19483.066058563 [ sid 59 start 19483.057050043 ] clnt 1:2 srv 2:2(0) #pages: 1 #objects: 1 total: 3266B seconds: 0.00900852 SUCCESS
19908.433161708 [ sid 60 start 19594.649094295 ] clnt 1:2 srv 2:2(0) #pages: 8 #objects: 12 total: 76468B seconds: 313.784067413 SUCCESS
------------------------------------------------------------------
| 1 timelines, 5 barriers, 280576 events, 1453 ms, 204 Kevt/s
------------------------------------------------------------------
```

Figura 22 Paquetes recibidos en el Servidor HTTP sin Congestión. BGP-4 Escenario 2.

La congestión es un fenómeno intrínseco de las redes de telecomunicaciones que afecta directamente el desempeño, esto se puede ver en la *Figura 23*, donde al protocolo de enrutamiento BGP-4 se le agrega un congestión total de ruta, que conlleva a una pérdida de paquetes significativa ya que ahora únicamente le están llegando 8 paquetes de los 61 enviados equivalentes a 578.233 bytes.

```
578.780652741 [ sid 0 start 60.416673721 ] clnt 1:2 srv 2:2(0) #pages: 2 #objects: 2 total: 11083B seconds: 518.36397902 SUCCESS
770.420144172 [ sid 1 start 588.49176388 ] clnt 1:2 srv 2:2(0) #pages: 1 #objects: 1 total: 3229B seconds: 181.928380292 SUCCESS
2774.071910124 [ sid 2 start 777.70423483 ] clnt 1:2 srv 2:2(0) #pages: 2 #objects: 3 total: 332547B seconds: 1996.367675294 SUCCESS
4378.688503755 [ sid 3 start 2816.168918617 ] clnt 1:2 srv 2:2(0) #pages: 2 #objects: 7 total: 34901B seconds: 1562.519585138 SUCCESS
4642.270945978 [ sid 4 start 4399.697538492 ] clnt 1:2 srv 2:2(0) #pages: 1 #objects: 1 total: 9138B seconds: 242.573407486 SUCCESS
5161.578672304 [ sid 5 start 4919.006651841 ] clnt 1:2 srv 2:2(0) #pages: 1 #objects: 1 total: 7360B seconds: 242.572020463 SUCCESS
12611.047367112 [ sid 6 start 5249.599441958 ] clnt 1:2 srv 2:2(0) #pages: 16 #objects: 32 total: 137513B seconds: 7361.447925154 SUCCESS
14783.993124097 [ sid 7 start 12660.268505973 ] clnt 1:2 srv 2:2(0) #pages: 7 #objects: 9 total: 42462B seconds: 2123.724618124 SUCCESS
------------------------------------------------------------------
| 1 timelines, 5 barriers, 269440 events, 1110 ms, 257 Kevt/s
------------------------------------------------------------------
```

Figura 23 Paquetes recibidos en el Servidor HTTP con Congestión. BGP-4. Escenario 2

3.2.2.2 Escenario2: BGP-C2 en t1

La *Figura 24*, muestra la tabla de enrutamiento del equipo R1 del AS1, en la cual se observa que la ruta 1 fue la seleccionada para llevar la información hasta el AS2, pero esta vez basada en el algoritmo de decisión de BGP-C2 (ver *Tabla 13*). La selección de la interfaz de salida, se

hace a través del atributo LOCAL_PREFERENCE asociado a un bajo costo de ruta y a un bajo grado de congestión como de pérdida de información.

```
.....................................................................
.........................   bgp@1:1 wrap-up   .........................
.....................................................................
~# 1:1   --- Loc-RIB at bgp@1:1:
~# 1:1  |      NetworkNHI         NextHopNHI       Metric LocPrf Weight ASPathNHI
~# 1:1  | *>   3                   2:1(2)                -    100      - 2 3
~# 1:1  | *>   2                   2:1(2)                -    100      - 2
~# 1:1  | *>   1                   self                  -      -      -           i

.....................................................................
```

Figura 24 Tabla de Enrutamiento R1 presente en AS1. Protocolo BGP-C2 en t1. Escenario 2.

Tabla 13 Congestión presente en cada Ruta. Escenario2 BGP-C2 en t1

Ruta	Congestión	P. Perdidos	B. Perdidos
Ruta1	0.16	10	1.024.662
Ruta2	0.46	28	5.397.199

3.2.2.2.1 Gráficas de Paquetes y Bytes Perdidos vs Tasa de Pérdida. BGP-C2

La *Tabla 14* y *Tabla 15*, indica el número de paquetes y bytes perdidos para diferentes valores de congestión durante la transmisión de información desde el R1 del AS1 al R1 del AS2. La ruta seleccionada por el BGP-C2 en este caso es la misma que toma BGP-4 por defecto, pero basada en el criterio de decisión de congestión y no en el del número de enlaces entre origen y destino.

Tabla 14 Paquetes Perdidos vs Tasa de Pérdida en la Ruta1. Escenario2 BGP-C2

Escenario2_BGP-C2		
P. Recibidos	**P. Perdidos**	**Tasa Pérdida**
57	0	0%
56	1	1.75%
54	3	5.26%
47	10	17.54%
44	13	22.81%
34	23	40.35%

En la *Figura 25* y *Figura26*, se observan los paquetes y los bytes perdidos respectivamente, para diferentes valores de congestión para la ruta seleccionada por el algoritmo de BGP-C2. La cantidad de paquetes de información que se envía es igual a la que se envía en el BGP-4. Se puede notar como a medida de que la tasa de pérdida crece, el valor de los paquetes y bytes perdidos aumenta de manera impredecible.

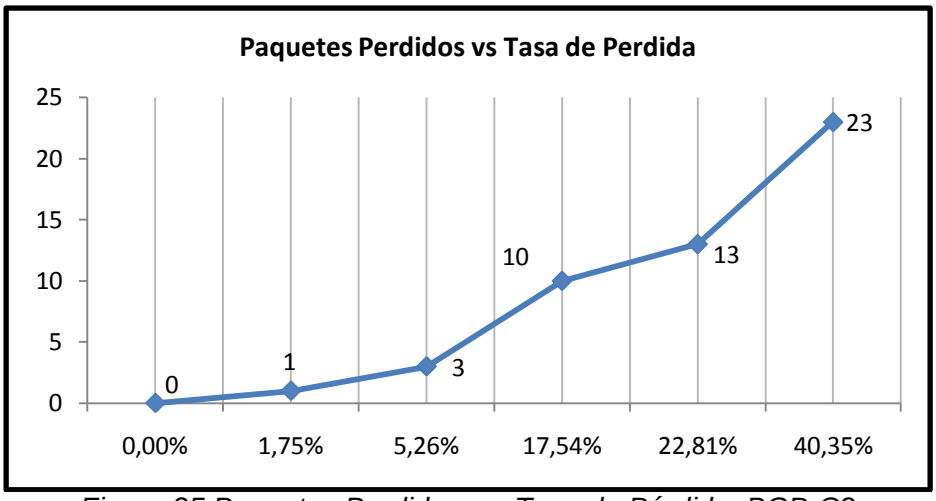

Figura 25 Paquetes Perdidos vs. Tasa de Pérdida. BGP-C2

Tabla 15 Bytes Perdidos vs Tasa de Pérdida en la Ruta1. Escenario2 BGP-C2

Escenario2_BGP-C2		
B. Recibidos	**B. Perdidos**	**Tasa Pérdida**
8,609,218	0	0%
8,395,042	214,176	2.49%
8,143,829	465,389	5.41%
7,764,741	844,477	9.81%
5,031,079	3,578,139	41.56%
4,282,038	4,327,180	50.26%

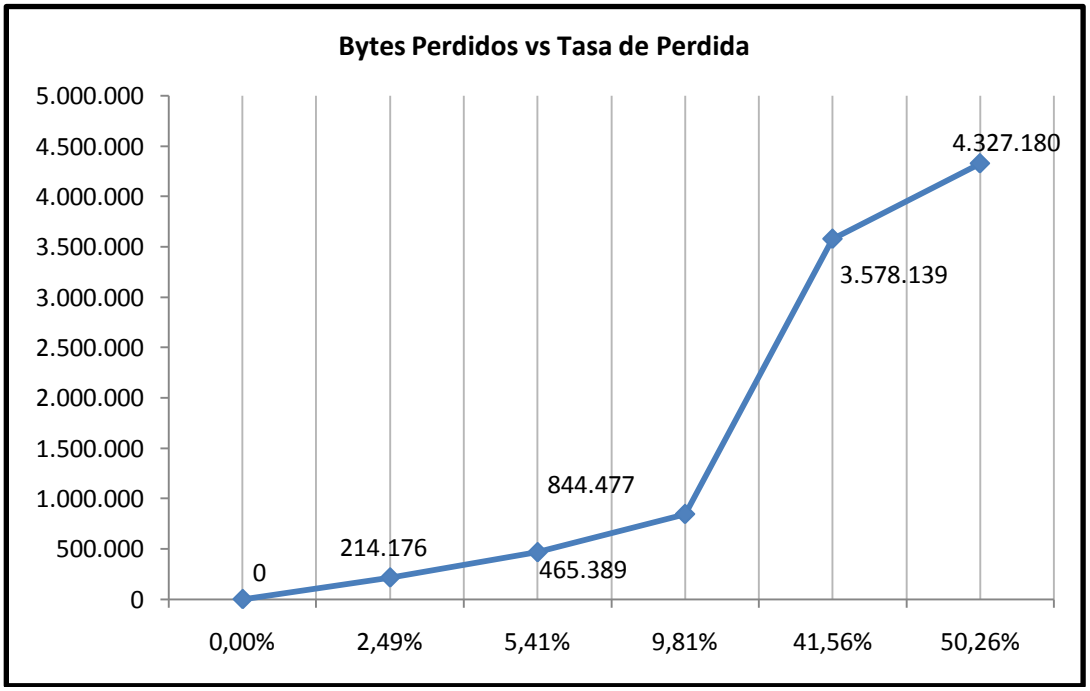

Figura 26 Bytes Perdidos vs. Tasa de Pérdida. BGP-C2

3.2.2.3 Escenario2: BGP-C2 en t2

La tabla de enrutamiento del R1 del AS1 que se observa en a *Figura 27*, muestra que la ruta2 es la seleccionada por el protocolo BGP-C2. Esta presenta una conexión indirecta a través del AS3 por lo que se puede notar en la *Figura 6,* donde se observan 3 saltos, dos inter-dominio y un intra-dominio. A pesar de ser la ruta más larga presenta menos pérdida de información debido a que la ruta1 está más congestionada (ver *Tabla 16*). Algo importante que se puede ver en la grafica son las tablas de enrutamiento del R1 del AS3, la cual indica que el próximo salto es R2 presente en el mismo dominio (enlace intra-dominio) y la tabla del R2 del mismo dominio que indica que su próximo salto es el R1 del AS2 donde se encuentre el destino.

```
.....................................................................
.........................   bgp@1:1 wrap-up   .........................
.....................................................................
~# 1:1   --- Loc-RIB at bgp@1:1:
~# 1:1  |      NetworkNHI         NextHopNHI       Metric LocPrf Weight ASPathNHI
~# 1:1  | *>   3                   3:1(1)                -    100      - 3
~# 1:1  | *>   2                   3:1(1)                -    100      - 3 2
~# 1:1  | *>   1                   self                  -      -      -           i

.....................................................................
.........................   bgp@3:1 wrap-up   .........................
.....................................................................
~# 3:1   --- Loc-RIB at bgp@3:1:
~# 3:1  |      NetworkNHI         NextHopNHI       Metric LocPrf Weight ASPathNHI
~# 3:1  | *>   3                   self                  -      -      -           i
~# 3:1  | *>   2                   3:2(1)                -      -      - 2         i
~# 3:1  | *>   1                   1:1(1)                -      -      - 1

.....................................................................
.........................   bgp@3:2 wrap-up   .........................
.....................................................................
~# 3:2   --- Loc-RIB at bgp@3:2:
~# 3:2  |      NetworkNHI         NextHopNHI       Metric LocPrf Weight ASPathNHI
~# 3:2  | *>   3                   self                  -      -      -           i
~# 3:2  | *>   2                   2:1(1)                -      -      - 2
~# 3:2  | *>   1                   3:1(2)                -      -      - 1         i

.....................................................................
```

Figura 27 Tabla de Enrutamiento R1 presente en el AS1. Protocolo BGP-C2 en t2 Escenario 2.

Tabla 16 Congestión presente en cada Ruta. Escenario 2 BGP-C2 en t2

Ruta	Congestión	P. Perdidos	B. Perdidos
Ruta1	0.23	13	3.578.139
Ruta2	0.05	3	465.389

3.2.2.3.1 Gráfica de Paquetes y Bytes Perdidos vs Tasa de Pérdida. BGP-C2

La *Tabla 17* y *Tabla 18* indica el número de paquetes y bytes perdidos entre el cliente HTTP y el servidor HTTP para diferentes valores de congestión. El algoritmo de decisión de BGP-C2 toma la ruta menos congestionada a pesar de ser la más larga.

Tabla 17 Paquetes Perdidos vs Tasa de Pérdida en la Ruta2. Escenario2 BGP-C2

Escenario2_BGP-C2		
P. Recibidos	**P. Perdidos**	**Tasa de Pérdida**
57	0	0%
56	1	1.75%
54	3	5.26%
44	13	22.81%
29	28	49.12%

La *Figura 28*, corresponde a los datos reunidos en la *Tabla 17*.

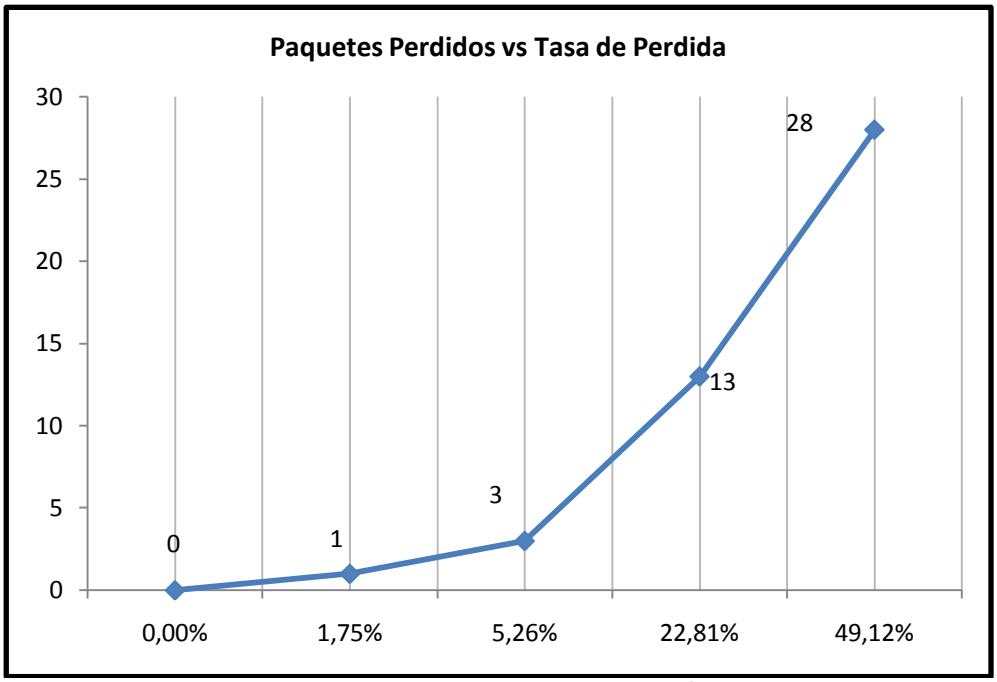

Figura 28 Paquetes Perdidos vs. Tasa de Pérdida. BGP-C2

Tabla 18 Bytes Perdidos vs Tasa de Pérdida en la Ruta2. Escenario2 BGP-C2

Escenario2_BGP-C2		
B. Recibidos	**B. Perdidos**	**Tasa de Pérdida**
8,609,218	0	0%
8,395,042	214,176	2.49%
8,143,829	465,389	5.41%
5,031,079	3,578,139	41.56%
3,131,641	5,477,577	63.62%

La *Figura 29*, corresponde a los datos reunidos en la *Tabla 18*.

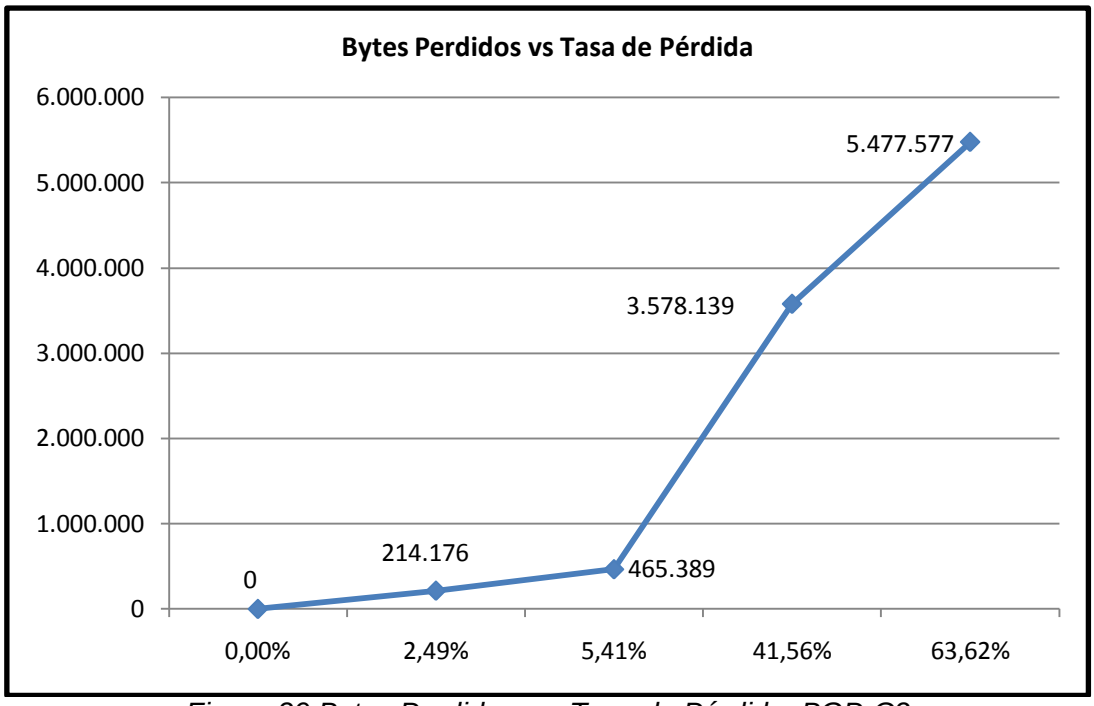

Figura 29 Bytes Perdidos vs. Tasa de Pérdida. BGP-C2

3.2.3 Escenario 3

3.2.3.1 Escenario3: BGP-4

La tabla de enrutamiento de la *Figura 30*, muestra que la ruta1 es la seleccionada por BGP-4 para el envío de información desde el R2 del AS1 al que se encuentra conectado el cliente HTTP hasta el R2 del AS2 al que se encuentra conectado el servidor HTTP. Aunque el número de saltos inter-dominio es el mismo, los saltos intra-dominio presentes en la ruta2 hacen que el valor del AS-Path se incremente, por tanto el algoritmo de decisión, toma como premisa la ruta1 por ser la que menos enlaces presenta, representado en el menor valor de métrica.

```
.....................................................................
.........................   bgp@1:1 wrap-up   .........................
.....................................................................
~# 1:1   --- Loc-RIB at bgp@1:1:
~# 1:1  |      NetworkNHI         NextHopNHI       Metric LocPrf Weight ASPathNHI
~# 1:1  | *>   2                   2:1(1)                -      -      - 2
~# 1:1  | *>   1                   self                  -      -      -           i

.....................................................................
.........................   bgp@1:2 wrap-up   .........................
.....................................................................
~# 1:2   --- Loc-RIB at bgp@1:2:
~# 1:2  |      NetworkNHI         NextHopNHI       Metric LocPrf Weight ASPathNHI
~# 1:2  | *>   2                   2:2(2)                -      -      - 2
~# 1:2  | *>   1                   self                  -      -      -           i

.....................................................................
```

Figura 30 Tabla de Enrutamiento R1 presente en el AS1. Protocolo BGP-4 Escenario 3.

Como para las topologías de red anteriores, este modelo no presenta ningún grado de congestión, con el objetivo de determinar la máxima cantidad de paquetes y bytes que llegan al destino. Para este caso el número de paquetes enviados como recibidos corresponde a 58 representados en 6.805.731 bytes como se muestra en la *Figura 31*.

```
271.931086861 [ sid 0 start 208.902776294 ] clnt 1:3 srv 2:3(0) #pages: 2 #objects: 2 total: 10931B seconds: 63.028310567 SUCCESS
395.150875659 [ sid 1 start 303.240929394 ] clnt 1:3 srv 2:3(0) #pages: 3 #objects: 5 total: 55443B seconds: 91.909946265 SUCCESS
1382.76955629 [ sid 2 start 432.392876282 ] clnt 1:3 srv 2:3(0) #pages: 18 #objects: 48 total: 206334B seconds: 950.376680008 SUCCESS
1434.859283673 [ sid 3 start 1408.355411375 ] clnt 1:3 srv 2:3(0) #pages: 1 #objects: 6 total: 60264B seconds: 26.503872298 SUCCESS
2334.072233632 [ sid 4 start 1441.643697657 ] clnt 1:3 srv 2:3(0) #pages: 17 #objects: 32 total: 159035B seconds: 892.428535975 SUCCESS
2929.625811044 [ sid 5 start 2402.699984532 ] clnt 1:3 srv 2:3(0) #pages: 9 #objects: 15 total: 77848B seconds: 526.925826512 SUCCESS
3144.673618842 [ sid 6 start 3029.266012793 ] clnt 1:3 srv 2:3(0) #pages: 4 #objects: 7 total: 22907B seconds: 115.407606049 SUCCESS
3323.743508275 [ sid 7 start 3320.735831414 ] clnt 1:3 srv 2:3(0) #pages: 1 #objects: 1 total: 2307B seconds: 3.007676861 SUCCESS
3394.137057146 [ sid 8 start 3391.129225408 ] clnt 1:3 srv 2:3(0) #pages: 1 #objects: 1 total: 2510B seconds: 3.007831738 SUCCESS
3997.973974181 [ sid 9 start 3883.730515318 ] clnt 1:3 srv 2:3(0) #pages: 4 #objects: 4 total: 25095B seconds: 114.243458863 SUCCESS
4269.522026165 [ sid 10 start 4007.875623868 ] clnt 1:3 srv 2:3(0) #pages: 6 #objects: 7 total: 32423B seconds: 261.646402297 SUCCESS
4523.411589841 [ sid 11 start 4309.748576431 ] clnt 1:3 srv 2:3(0) #pages: 6 #objects: 11 total: 70697B seconds: 213.66301341 SUCCESS
4941.810999707 [ sid 12 start 4675.789878564 ] clnt 1:3 srv 2:3(0) #pages: 7 #objects: 8 total: 38679B seconds: 266.021121143 SUCCESS
5344.601852842 [ sid 13 start 5013.396357826 ] clnt 1:3 srv 2:3(0) #pages: 7 #objects: 7 total: 142388B seconds: 331.205495016 SUCCESS
5579.257477701 [ sid 14 start 5576.248722043 ] clnt 1:3 srv 2:3(0) #pages: 1 #objects: 1 total: 3721B seconds: 3.008755658 SUCCESS
5596.672590067 [ sid 15 start 5592.661999041 ] clnt 1:3 srv 2:3(0) #pages: 1 #objects: 1 total: 5775B seconds: 4.010591026 SUCCESS
5899.559432021 [ sid 16 start 5895.549994017 ] clnt 1:3 srv 2:3(0) #pages: 1 #objects: 1 total: 5057B seconds: 4.009438004 SUCCESS
6105.309567634 [ sid 17 start 6042.116716542 ] clnt 1:3 srv 2:3(0) #pages: 2 #objects: 9 total: 38978B seconds: 63.192851092 SUCCESS
6325.229618864 [ sid 18 start 6120.094484506 ] clnt 1:3 srv 2:3(0) #pages: 5 #objects: 7 total: 41612B seconds: 205.135134358 SUCCESS
7204.33405804 [ sid 19 start 6371.789707615 ] clnt 1:3 srv 2:3(0) #pages: 13 #objects: 77 total: 489383B seconds: 832.544350425 SUCCESS
7689.879767725 [ sid 20 start 7301.236661355 ] clnt 1:3 srv 2:3(0) #pages: 8 #objects: 34 total: 1394852B seconds: 388.64310637 SUCCESS
8559.16261476 [ sid 21 start 8055.548958823 ] clnt 1:3 srv 2:3(0) #pages: 7 #objects: 29 total: 169536B seconds: 503.613655937 SUCCESS
8987.454590123 [ sid 22 start 8904.976360893 ] clnt 1:3 srv 2:3(0) #pages: 3 #objects: 4 total: 202043B seconds: 82.47822923 SUCCESS
9088.745258719 [ sid 23 start 9083.729629366 ] clnt 1:3 srv 2:3(0) #pages: 1 #objects: 1 total: 15450B seconds: 5.015629353 SUCCESS
9519.996765136 [ sid 24 start 9203.828801288 ] clnt 1:3 srv 2:3(0) #pages: 7 #objects: 26 total: 520140B seconds: 316.167963848 SUCCESS
9574.797339329 [ sid 25 start 9568.595206479 ] clnt 1:3 srv 2:3(0) #pages: 1 #objects: 2 total: 5544B seconds: 6.20213285 SUCCESS
9731.56757512 [ sid 26 start 9645.603263433 ] clnt 1:3 srv 2:3(0) #pages: 3 #objects: 4 total: 14470B seconds: 85.964311687 SUCCESS
10463.039157212 [ sid 27 start 10148.736491284 ] clnt 1:3 srv 2:3(0) #pages: 7 #objects: 10 total: 49809B seconds: 314.302665928 SUCCESS
10617.242979804 [ sid 28 start 10464.197707869 ] clnt 1:3 srv 2:3(0) #pages: 3 #objects: 4 total: 51113B seconds: 153.045271935 SUCCESS
10745.515803431 [ sid 29 start 10679.70069274 ] clnt 1:3 srv 2:3(0) #pages: 2 #objects: 6 total: 32369B seconds: 65.815110691 SUCCESS
11552.009521501 [ sid 30 start 11046.453196246 ] clnt 1:3 srv 2:3(0) #pages: 9 #objects: 21 total: 212702B seconds: 505.556325255 SUCCESS
11851.147563293 [ sid 31 start 11761.618337295 ] clnt 1:3 srv 2:3(0) #pages: 3 #objects: 5 total: 31825B seconds: 89.529225998 SUCCESS
12179.172152692 [ sid 32 start 11919.026286522 ] clnt 1:3 srv 2:3(0) #pages: 6 #objects: 6 total: 61588B seconds: 260.14586617 SUCCESS
12758.206605692 [ sid 33 start 12217.326307384 ] clnt 1:3 srv 2:3(0) #pages: 11 #objects: 28 total: 135744B seconds: 540.880298308 SUCCESS
12846.490348294 [ sid 34 start 12806.005286605 ] clnt 1:3 srv 2:3(0) #pages: 2 #objects: 2 total: 13734B seconds: 40.485061689 SUCCESS
13067.527276584 [ sid 35 start 12903.382302423 ] clnt 1:3 srv 2:3(0) #pages: 4 #objects: 15 total: 279592B seconds: 164.144974161 SUCCESS
13233.782159511 [ sid 36 start 13141.177345632 ] clnt 1:3 srv 2:3(0) #pages: 3 #objects: 5 total: 129799B seconds: 92.604813879 SUCCESS
13369.223096077 [ sid 37 start 13333.582597816 ] clnt 1:3 srv 2:3(0) #pages: 2 #objects: 2 total: 23575B seconds: 35.640498261 SUCCESS
14877.490907164 [ sid 38 start 13463.758687154 ] clnt 1:3 srv 2:3(0) #pages: 22 #objects: 83 total: 459043B seconds: 1413.73222001 SUCCESS
15008.416358476 [ sid 39 start 14923.739923402 ] clnt 1:3 srv 2:3(0) #pages: 3 #objects: 5 total: 23047B seconds: 84.676435074 SUCCESS
15036.000430523 [ sid 40 start 15010.350022648 ] clnt 1:3 srv 2:3(0) #pages: 1 #objects: 7 total: 31551B seconds: 25.650407875 SUCCESS
15282.248383379 [ sid 41 start 15209.649336475 ] clnt 1:3 srv 2:3(0) #pages: 2 #objects: 2 total: 5724B seconds: 72.599046904 SUCCESS
15360.105665863 [ sid 42 start 15317.222933844 ] clnt 1:3 srv 2:3(0) #pages: 2 #objects: 2 total: 6086B seconds: 42.882732019 SUCCESS
16138.212269454 [ sid 43 start 15458.464977904 ] clnt 1:3 srv 2:3(0) #pages: 8 #objects: 49 total: 306349B seconds: 679.74729155 SUCCESS
16169.547488667 [ sid 44 start 16160.276918084 ] clnt 1:3 srv 2:3(0) #pages: 1 #objects: 2 total: 35439B seconds: 9.270570583 SUCCESS
16291.132431494 [ sid 45 start 16287.122211426 ] clnt 1:3 srv 2:3(0) #pages: 1 #objects: 1 total: 5544B seconds: 4.010220068 SUCCESS
16369.093762315 [ sid 46 start 16337.822981361 ] clnt 1:3 srv 2:3(0) #pages: 1 #objects: 8 total: 56494B seconds: 31.270780954 SUCCESS
16614.090432048 [ sid 47 start 16372.211462545 ] clnt 1:3 srv 2:3(0) #pages: 4 #objects: 11 total: 57224B seconds: 241.878969503 SUCCESS
16928.007528259 [ sid 48 start 16656.799832402 ] clnt 1:3 srv 2:3(0) #pages: 4 #objects: 7 total: 24092B seconds: 271.207695857 SUCCESS
17621.6021278 [ sid 49 start 16929.94524325 ] clnt 1:3 srv 2:3(0) #pages: 12 #objects: 17 total: 118474B seconds: 691.65688455 SUCCESS
18857.984776808 [ sid 50 start 17685.518949782 ] clnt 1:3 srv 2:3(0) #pages: 23 #objects: 42 total: 396711B seconds: 1172.465827026 SUCCESS
18922.351287825 [ sid 51 start 18868.717721428 ] clnt 1:3 srv 2:3(0) #pages: 2 #objects: 2 total: 38347B seconds: 53.633566397 SUCCESS
18969.040990524 [ sid 52 start 18955.449976115 ] clnt 1:3 srv 2:3(0) #pages: 1 #objects: 3 total: 58702B seconds: 13.591014409 SUCCESS
19120.110711473 [ sid 53 start 19053.705914834 ] clnt 1:3 srv 2:3(0) #pages: 2 #objects: 2 total: 9069B seconds: 66.404796639 SUCCESS
19249.531049353 [ sid 54 start 19244.514593737 ] clnt 1:3 srv 2:3(0) #pages: 1 #objects: 1 total: 16493B seconds: 5.016455616 SUCCESS
19318.554535639 [ sid 55 start 19269.160516751 ] clnt 1:3 srv 2:3(0) #pages: 2 #objects: 5 total: 26717B seconds: 49.394018888 SUCCESS
19500.788251346 [ sid 56 start 19497.78058364 ] clnt 1:3 srv 2:3(0) #pages: 1 #objects: 1 total: 2295B seconds: 3.007667706 SUCCESS
19972.902714954 [ sid 57 start 19557.762503814 ] clnt 1:3 srv 2:3(0) #pages: 8 #objects: 35 total: 293058B seconds: 415.14021114 SUCCESS
----------------------------------------------------------------------
| 1 timelines, 5 barriers, 276002 events, 1406 ms, 207 Kevt/s
----------------------------------------------------------------------
```

Figura 31 Paquetes recibidos en el Servidor HTTP sin Congestión. BGP-4 Escenario 3.

Una forma de cuantificar el efecto de la congestión en una red IP, es precisamente considerando la relación de la información recibida con respecto a la enviada; esta permite determinar la forma en la que el desempeño de la red se ve afectado. Para lo anterior se genera congestión de ruta, esta ocasiona una pérdida de 54 paquetes equivalentes a 6.472.759 como se muestra en la *Figura 32.*

```
775.932643257 [ sid 0 start 208.902776294 ] clnt 1:3 srv 2:3(0) #pages: 2 #objects: 2 total: 10931B seconds: 567.029866963 SUCCESS
2703.175931335 [ sid 1 start 807.24248579 ] clnt 1:3 srv 2:3(0) #pages: 3 #objects: 5 total: 55443B seconds: 1895.933445545 SUCCESS
15862.854649189 [ sid 2 start 2740.417931958 ] clnt 1:3 srv 2:3(0) #pages: 18 #objects: 48 total: 206334B seconds: 13122.436717231 SUCCESS
18006.974310155 [ sid 3 start 15888.440504274 ] clnt 1:3 srv 2:3(0) #pages: 1 #objects: 6 total: 60264B seconds: 2118.533805881 SUCCESS
----------------------------------------------------------------------
| 1 timelines, 5 barriers, 267741 events, 1109 ms, 251 Kevt/s
----------------------------------------------------------------------
```

Figura 32 Paquetes recibidos en el Servidor HTTP con Congestión. BGP-4 Escenario 3

3.2.3.2 Escenario3: BGP-C2 en t1

La *Figura 33* muestra la tabla de enrutamiento del R2 del AS1, enrutador al que se encuentra conectado el cliente HTTP; en ésta se observa que la ruta seleccionada por el protocolo BGP-C2 es la ruta1, la misma que tomo el BGP-4, con la diferencia que para este caso el algoritmo considera como criterio de decisión la congestión presente a lo largo de las rutas (ver *Tabla 19*). La interfaz de salida se escoge mediante un valor alto (100) en el atributo LOCAL_PREFERENCE, el cual está asociado a un bajo costo de ruta y a una baja congestión, que implica una menor pérdida de paquetes.

```
.....................................................................
.....................|.......   bgp@1:1 wrap-up   ....................
.....................................................................
~# 1:1   --- Loc-RIB at bgp@1:1:
~# 1:1  |      NetworkNHI         NextHopNHI       Metric LocPrf Weight ASPathNHI
~# 1:1  | *>   2                   1:2(1)                -    100      - 2          i
~# 1:1  | *>   1                   self                  -      -      -            i

.....................................................................
.........................   bgp@1:2 wrap-up   ........................
.....................................................................
~# 1:2   --- Loc-RIB at bgp@1:2:
~# 1:2  |      NetworkNHI         NextHopNHI       Metric LocPrf Weight ASPathNHI
~# 1:2  | *>   2                   2:2(2)                -    100      - 2
~# 1:2  | *>   1                   self                  -      -      -            i

.....................................................................
```

Figura 33 Tabla de Enrutamiento de R2 presente en el AS1. BGP-C2 en t1 Escenario 3.

Tabla 19 Congestión presente en cada Ruta. Escenario 3 BGP-C2 en t1

Ruta	Congestión	P. Perdidos	B. Perdidos
Ruta1	0.10	6	406.334
Ruta2	0.29	17	1.456.818

3.2.3.2.1 Grafica de Paquetes Bytes Perdidos vs Índice de Pérdida.

La *Tabla 20* y la *Tabla 21,* muestran la cantidad de paquetes y de bytes perdidos en diferentes ejecuciones del protocolo BGP-C2 (ver *Figura 34* y *Figura 35)*. El algoritmo de decisión de dicho protocolo toma la ruta1, considerando que esta presenta una menor congestión total que la ruta2.

Tabla 20 Paquetes Perdidos vs Tasa de Pérdida en la Ruta1. Escenario 3 BGPC-2

Escenario3_BGP-C2		
P. Recibidos	**P. Perdidos**	**Tasa de pérdida**
58	0	0%
54	4	6.90%
43	15	25.86%
40	18	31.03%
22	36	62.07%

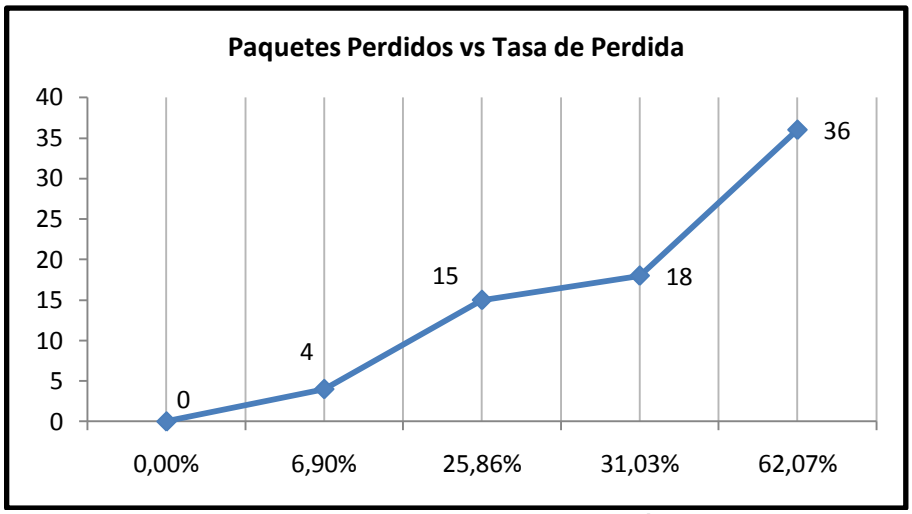

Figura 34 Paquetes Perdidos vs. Tasa de Pérdida. BGP-C2

Tabla 21 Bytes Perdidos vs Tasa de Pérdida en la Ruta1. Escenario 3 BGP-C2

Escenario1_BGP-C2		
B. Recibidos	**B. Perdidos**	**Tasa de Pérdida**
6,805,731	0	0%
6,467,168	338,563	4.97%
5,360,723	1,445,008	21.23%
5,317,362	1,488,369	21.87%
3,055,775	3,749,956	55.10%

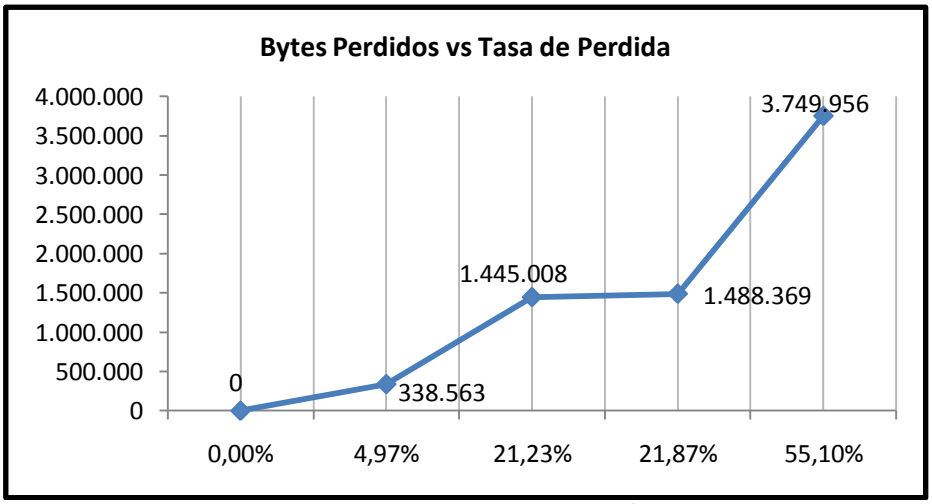

Figura 35 Bytes Perdidos vs. Tasa de Pérdida. BGP-C2

3.2.3.3 Escenario3: BGP-C2 en t2

La tabla de enrutamiento del R2 del AS1 que se muestra en la *Figura 36*, indica que la ruta seleccionada por el algoritmo de decisión de BGP-C2 es la presenta el primer salto hacia el R1 de su mismo dominio (ver *Tabla 22*), esta ruta presenta en tres saltos, dos intra-dominio

y un inter-dominio. Lamentablemente por limitaciones del simulador la tabla de enrutamiento no muestra un salto dentro de un mismo dominio destino, únicamente expresa mediante el NextHopNHI que el salto se realiza dentro del AS con la palabra “self”, pero cabe resaltar que la entrada al dominio destino es la interfaz1 del R1 del AS2 según la dirección NHI. Para la selección de la interfaz de salida del R2 del AS1 para el envío de información se hace uso del atributo LOCAL_PREFERENCE, que está representado por un valor de 100, éste se asocia a un bajo costo de ruta, el cual representa con un bajo grado de congestión y por ende una menor pérdida de paquetes.

```
.....................................................................
.........................   bgp@1:1 wrap-up   .........................
.....................................................................
~# 1:1   --- Loc-RIB at bgp@1:1:
~# 1:1  |      NetworkNHI         NextHopNHI       Metric LocPrf Weight ASPathNHI
~# 1:1  | *>   2                   2:1(1)                -    100      - 2
~# 1:1  | *>   1                   self                  -      -      -           i

.....................................................................
.........................   bgp@1:2 wrap-up   .........................
.....................................................................
~# 1:2   --- Loc-RIB at bgp@1:2:
~# 1:2  |      NetworkNHI         NextHopNHI       Metric LocPrf Weight ASPathNHI
~# 1:2  | *>   2                   1:1(2)                -    100      - 2         i
~# 1:2  | *>   1                   self                  -      -      -           i

.....................................................................
```

Figura 36 Tabla de Enrutamiento de R2 presente en el AS1. BGP-C2 en t2 Escenario 3.

Tabla 22 Congestión presente en cada Ruta. Escenario 3. BGP-C2 en t2

Ruta	Congestión	P. Perdidos	B. Perdidos
Ruta1	0.10	6	406.334
Ruta2	0.29	17	1.456.818

3.2.3.3.1 Grafica de Paquetes y Bytes Perdidos vs Tasa de Pérdida.

La *Tabla 23* y *Tabla 24,* muestran la cantidad de paquetes y bytes perdidos en una transmisión entre cliente HTTP y servidor HTTP (ver *Figura 37* y *Figura 38*). La ruta2 es la seleccionada por BGP-C2, por presentar una menor congestión de ruta, lo que implica una menor pérdida de paquetes de información.

Tabla 23 Paquetes Perdidos vs Tasa de Pérdida en la Ruta2. Escenario 3 BGP-C2

Escenario3_BGP-C2		
P. Recibidos	**P. Pérdidas**	**Tasa de Pérdida**
58	0	0%
54	4	6.90%
47	11	18.97%
40	18	31.03%
31	27	46.55%
19	39	67.24%

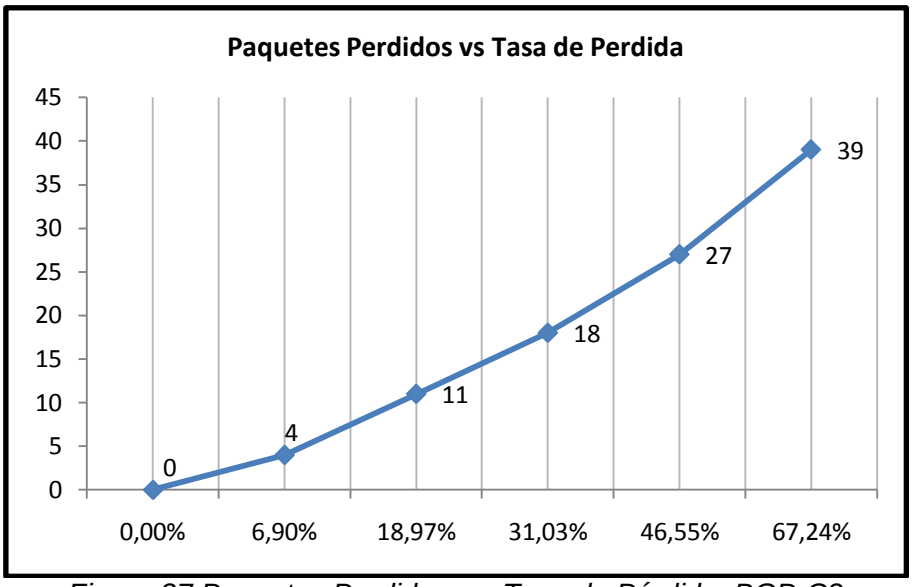

Figura 37 Paquetes Perdidos vs. Tasa de Pérdida. BGP-C2

Tabla 24 Bytes Perdidos vs Tasa de Pérdida en la Ruta2. Escenario 3 BGP-C2

Escenario3_BGP-C2		
B. Recibidos	**B. Perdidos**	**Tasa de Pérdida**
6,805,731	0	0%
6,467,168	338,563	4.97%
5,764,549	1,041,182	15.30%
5,317,362	1,488,369	21.87%
4,159,415	2,646,316	38.88%
1,002,004	5,803,727	85.28%

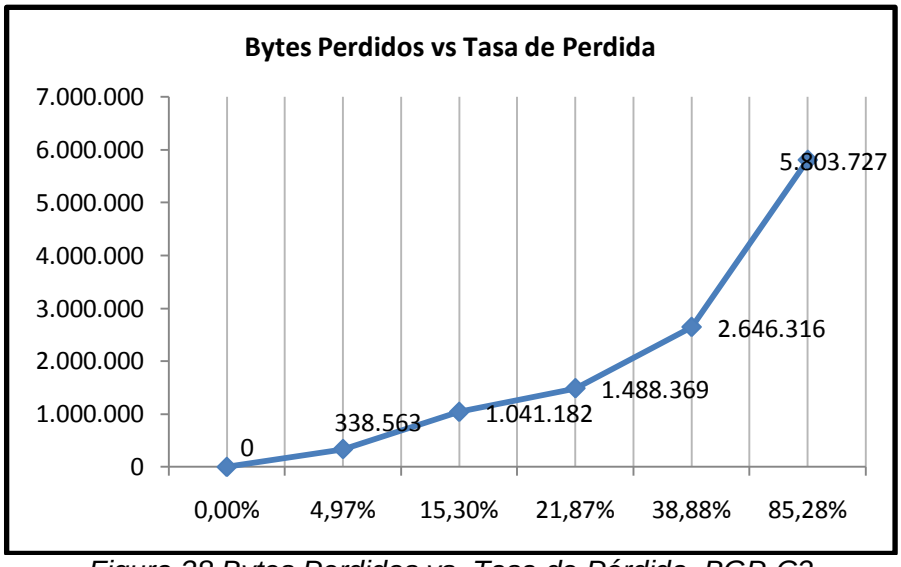

Figura 38 Bytes Perdidos vs. Tasa de Pérdida. BGP-C2

3.2.4 Escenario4

3.2.4.1 Escenario4: BGP-4

La *Figura 39*, indica la tabla de enrutamiento del R1 del AS1 al cual se encuentra conectado el cliente HTTP; esta nos muestra que para enviar paquetes de información hacia el servidor HTTP, el criterio del menor número de enlaces no es suficiente para seleccionar la ruta, es necesario considerar los criterios de desempate de rutas mencionados en el Capítulo I; para este caso, la pauta para definir entre los posibles caminos se basa en la preferencia que tiene eBGP sobre iBGP, por tal razón, la ruta2 se elige por tener un enlace inter-dominio directo al AS destino, caso contario que la ruta1, la cual para llegar al servidor HTTP primero debe atravesar un enlace intra-dominio.

```
.....................................................................
.........................   bgp@1:1 wrap-up   .........................
.....................................................................
~# 1:1   --- Loc-RIB at bgp@1:1:
~# 1:1  |      NetworkNHI         NextHopNHI       Metric LocPrf Weight ASPathNHI
~# 1:1  | *>   2                   2:1(1)                -      -      - 2
~# 1:1  | *>   1                   self                  -      -      -           i

.....................................................................
.........................   bgp@1:2 wrap-up   .........................
.....................................................................
~# 1:2   --- Loc-RIB at bgp@1:2:
~# 1:2  |      NetworkNHI         NextHopNHI       Metric LocPrf Weight ASPathNHI
~# 1:2  | *>   2                   2:2(2)                -      -      - 2
~# 1:2  | *>   1                   self                  -      -      -           i

.....................................................................
```

Figura 39 Tabla de Enrutamiento R1 presente en el AS1 Protocolo BGP-4 Escenario 4.

Ahora bien, como en el escenario de simulación anterior se ejecuta BGP-4 sin considerar congestión, para así obtener una pérdida de paquetes de información de cero, lo que corresponde a 58 paquetes recibidos con una totalidad máxima de 6.805.731 bytes como se muestra en la *Figura 40*.

```
271.940543496 [ sid 0 start 208.902776294 ] clnt 1:3 srv 2:3(0) #pages: 2 #objects: 2 total: 10931B seconds: 63.037767202 SUCCESS
395.190228077 [ sid 1 start 303.250386029 ] clnt 1:3 srv 2:3(0) #pages: 3 #objects: 5 total: 55443B seconds: 91.939842048 SUCCESS
1383.018567206 [ sid 2 start 432.4322287 ] clnt 1:3 srv 2:3(0) #pages: 18 #objects: 48 total: 206334B seconds: 950.586338506 SUCCESS
1435.142214551 [ sid 3 start 1408.604422291 ] clnt 1:3 srv 2:3(0) #pages: 1 #objects: 6 total: 60264B seconds: 26.53779226 SUCCESS
2334.499507758 [ sid 4 start 1441.926628535 ] clnt 1:3 srv 2:3(0) #pages: 17 #objects: 32 total: 159035B seconds: 892.572879223 SUCCESS
2930.119666464 [ sid 5 start 2403.127258658 ] clnt 1:3 srv 2:3(0) #pages: 9 #objects: 15 total: 77848B seconds: 526.992407806 SUCCESS
3145.195398065 [ sid 6 start 3029.759868213 ] clnt 1:3 srv 2:3(0) #pages: 4 #objects: 7 total: 22907B seconds: 115.435529852 SUCCESS
3324.269122359 [ sid 7 start 3321.257610637 ] clnt 1:3 srv 2:3(0) #pages: 1 #objects: 1 total: 2307B seconds: 3.011511722 SUCCESS
3394.666506091 [ sid 8 start 3391.654839492 ] clnt 1:3 srv 2:3(0) #pages: 1 #objects: 1 total: 2510B seconds: 3.011666599 SUCCESS
3998.523718188 [ sid 9 start 3884.259964263 ] clnt 1:3 srv 2:3(0) #pages: 4 #objects: 4 total: 25095B seconds: 114.263753925 SUCCESS
4270.10157157 [ sid 10 start 4008.425367875 ] clnt 1:3 srv 2:3(0) #pages: 6 #objects: 7 total: 32423B seconds: 261.676203695 SUCCESS
4524.044310384 [ sid 11 start 4310.328121836 ] clnt 1:3 srv 2:3(0) #pages: 6 #objects: 11 total: 70697B seconds: 213.716188548 SUCCESS
4942.479495246 [ sid 12 start 4676.422599107 ] clnt 1:3 srv 2:3(0) #pages: 7 #objects: 8 total: 38679B seconds: 266.056896139 SUCCESS
5345.309700799 [ sid 13 start 5014.064853365 ] clnt 1:3 srv 2:3(0) #pages: 7 #objects: 7 total: 142388B seconds: 331.244847434 SUCCESS
5579.969160519 [ sid 14 start 5576.95657 ] clnt 1:3 srv 2:3(0) #pages: 1 #objects: 1 total: 3721B seconds: 3.012590519 SUCCESS
5597.389722998 [ sid 15 start 5593.373681859 ] clnt 1:3 srv 2:3(0) #pages: 1 #objects: 1 total: 5775B seconds: 4.016041139 SUCCESS
5900.281467274 [ sid 16 start 5896.267126948 ] clnt 1:3 srv 2:3(0) #pages: 1 #objects: 1 total: 5057B seconds: 4.014340326 SUCCESS
6106.071477375 [ sid 17 start 6042.838751795 ] clnt 1:3 srv 2:3(0) #pages: 2 #objects: 9 total: 38978B seconds: 63.23272558 SUCCESS
6326.023607486 [ sid 18 start 6120.856394247 ] clnt 1:3 srv 2:3(0) #pages: 5 #objects: 7 total: 41612B seconds: 205.167213239 SUCCESS
7205.486203809 [ sid 19 start 6372.583696237 ] clnt 1:3 srv 2:3(0) #pages: 13 #objects: 77 total: 489383B seconds: 832.902507572 SUCCESS
7691.214823874 [ sid 20 start 7302.388807124 ] clnt 1:3 srv 2:3(0) #pages: 8 #objects: 34 total: 1394852B seconds: 388.82601675 SUCCESS
8560.632965693 [ sid 21 start 8056.884014972 ] clnt 1:3 srv 2:3(0) #pages: 7 #objects: 29 total: 169536B seconds: 503.748950721 SUCCESS
8988.954575804 [ sid 22 start 8906.446711826 ] clnt 1:3 srv 2:3(0) #pages: 3 #objects: 4 total: 202043B seconds: 82.507863978 SUCCESS
9090.252653087 [ sid 23 start 9085.229615047 ] clnt 1:3 srv 2:3(0) #pages: 1 #objects: 1 total: 15450B seconds: 5.02303804 SUCCESS
9521.638693963 [ sid 24 start 9205.336195656 ] clnt 1:3 srv 2:3(0) #pages: 7 #objects: 26 total: 520140B seconds: 316.302498307 SUCCESS
9576.446937878 [ sid 25 start 9570.237135306 ] clnt 1:3 srv 2:3(0) #pages: 1 #objects: 2 total: 5544B seconds: 6.209802572 SUCCESS
9733.233978937 [ sid 26 start 9647.252861982 ] clnt 1:3 srv 2:3(0) #pages: 3 #objects: 4 total: 14470B seconds: 85.981116955 SUCCESS
10464.751290859 [ sid 27 start 10150.402895101 ] clnt 1:3 srv 2:3(0) #pages: 7 #objects: 10 total: 49809B seconds: 314.348395758 SUCCESS
10618.978331552 [ sid 28 start 10465.909841516 ] clnt 1:3 srv 2:3(0) #pages: 3 #objects: 4 total: 51113B seconds: 153.068490036 SUCCESS
10747.27838983 [ sid 29 start 10681.436044488 ] clnt 1:3 srv 2:3(0) #pages: 2 #objects: 6 total: 32369B seconds: 65.842345342 SUCCESS
11553.874915522 [ sid 30 start 11048.215782645 ] clnt 1:3 srv 2:3(0) #pages: 9 #objects: 21 total: 212702B seconds: 505.659132877 SUCCESS
11853.036695849 [ sid 31 start 11763.483731316 ] clnt 1:3 srv 2:3(0) #pages: 3 #objects: 5 total: 31825B seconds: 89.552964533 SUCCESS
12181.089655153 [ sid 32 start 11920.915419078 ] clnt 1:3 srv 2:3(0) #pages: 6 #objects: 6 total: 61588B seconds: 260.174236075 SUCCESS
12760.251670982 [ sid 33 start 12219.243809845 ] clnt 1:3 srv 2:3(0) #pages: 11 #objects: 28 total: 135744B seconds: 541.007861137 SUCCESS
12848.544870219 [ sid 34 start 12808.050351895 ] clnt 1:3 srv 2:3(0) #pages: 2 #objects: 2 total: 13734B seconds: 40.494518324 SUCCESS
13069.662437833 [ sid 35 start 12905.436824348 ] clnt 1:3 srv 2:3(0) #pages: 4 #objects: 15 total: 279592B seconds: 164.225613485 SUCCESS
13235.951194073 [ sid 36 start 13143.312506881 ] clnt 1:3 srv 2:3(0) #pages: 3 #objects: 5 total: 129799B seconds: 92.638687192 SUCCESS
13371.4051611 [ sid 37 start 13335.751632378 ] clnt 1:3 srv 2:3(0) #pages: 2 #objects: 2 total: 23575B seconds: 35.653528722 SUCCESS
14880.046709651 [ sid 38 start 13465.940752177 ] clnt 1:3 srv 2:3(0) #pages: 22 #objects: 83 total: 459043B seconds: 1414.105957474 SUCCESS
15010.993122181 [ sid 39 start 14926.295725889 ] clnt 1:3 srv 2:3(0) #pages: 3 #objects: 5 total: 23047B seconds: 84.697396292 SUCCESS
15038.608301887 [ sid 40 start 15012.926786353 ] clnt 1:3 srv 2:3(0) #pages: 1 #objects: 7 total: 31551B seconds: 25.681515534 SUCCESS
15284.863924465 [ sid 41 start 15212.257207839 ] clnt 1:3 srv 2:3(0) #pages: 2 #objects: 2 total: 5724B seconds: 72.606716626 SUCCESS
15362.728876671 [ sid 42 start 15319.83847493 ] clnt 1:3 srv 2:3(0) #pages: 2 #objects: 2 total: 6086B seconds: 42.890401741 SUCCESS
16141.061225556 [ sid 43 start 15461.088188712 ] clnt 1:3 srv 2:3(0) #pages: 8 #objects: 49 total: 306349B seconds: 679.973036844 SUCCESS
16172.40947523 [ sid 44 start 16163.125874186 ] clnt 1:3 srv 2:3(0) #pages: 1 #objects: 2 total: 35439B seconds: 9.283601044 SUCCESS
16293.999691931 [ sid 45 start 16289.984197989 ] clnt 1:3 srv 2:3(0) #pages: 1 #objects: 1 total: 5544B seconds: 4.015493942 SUCCESS
16371.999973211 [ sid 46 start 16340.690241798 ] clnt 1:3 srv 2:3(0) #pages: 1 #objects: 8 total: 56494B seconds: 31.309731413 SUCCESS
16617.045974067 [ sid 47 start 16375.117673441 ] clnt 1:3 srv 2:3(0) #pages: 4 #objects: 11 total: 57224B seconds: 241.928300626 SUCCESS
16930.992027865 [ sid 48 start 16659.755374421 ] clnt 1:3 srv 2:3(0) #pages: 4 #objects: 7 total: 24092B seconds: 271.236653444 SUCCESS
17624.669902142 [ sid 49 start 16932.929742856 ] clnt 1:3 srv 2:3(0) #pages: 12 #objects: 17 total: 118474B seconds: 691.740159286 SUCCESS
18861.255775342 [ sid 50 start 17688.586724124 ] clnt 1:3 srv 2:3(0) #pages: 23 #objects: 42 total: 396711B seconds: 1172.669051218 SUCCESS
18925.63531682 [ sid 51 start 18871.988719962 ] clnt 1:3 srv 2:3(0) #pages: 2 #objects: 2 total: 38347B seconds: 53.646596858 SUCCESS
18972.343671754 [ sid 52 start 18958.73400511 ] clnt 1:3 srv 2:3(0) #pages: 1 #objects: 3 total: 58702B seconds: 13.609666644 SUCCESS
19123.422391574 [ sid 53 start 19057.008596064 ] clnt 1:3 srv 2:3(0) #pages: 2 #objects: 2 total: 9069B seconds: 66.41379551 SUCCESS
19252.850138141 [ sid 54 start 19247.826273838 ] clnt 1:3 srv 2:3(0) #pages: 1 #objects: 1 total: 16493B seconds: 5.023864303 SUCCESS
19321.896372558 [ sid 55 start 19272.479605539 ] clnt 1:3 srv 2:3(0) #pages: 2 #objects: 5 total: 26717B seconds: 49.416767019 SUCCESS
19504.133923126 [ sid 56 start 19501.122420559 ] clnt 1:3 srv 2:3(0) #pages: 1 #objects: 1 total: 2295B seconds: 3.011502567 SUCCESS
19976.427268467 [ sid 57 start 19561.108175594 ] clnt 1:3 srv 2:3(0) #pages: 8 #objects: 35 total: 293058B seconds: 415.319092873 SUCCESS
-----------------------------------------------------------------
| 1 timelines, 5 barriers, 290332 events, 1578 ms, 191 Kevt/s
-----------------------------------------------------------------
```

Figura 40 Paquetes recibidos en el Servidor HTTP sin Congestión. BGP-4 Escenario 4.

En la *Figura 41* se puede ver el efecto que tiene la congestión sobre el desempeño de una red; este fenómeno está relacionado directamente con la pérdida de paquetes, por lo que a mayor congestión mayor pérdida de paquetes y viceversa. Los resultados muestran que se han perdido 54 paquetes de los 58 enviados lo que corresponde a 6.472.759 de bytes perdidos.

```
775.932643257 [ sid 0 start 208.902776294 ] clnt 1:3 srv 2:3(0) #pages: 2 #objects: 2 total: 10931B seconds: 567.029866963 SUCCESS
2703.175931335 [ sid 1 start 807.24248579 ] clnt 1:3 srv 2:3(0) #pages: 3 #objects: 5 total: 55443B seconds: 1895.933445545 SUCCESS
15862.854649189 [ sid 2 start 2740.417931958 ] clnt 1:3 srv 2:3(0) #pages: 18 #objects: 48 total: 206334B seconds: 13122.436717231 SUCCESS
18006.974310155 [ sid 3 start 15888.440504274 ] clnt 1:3 srv 2:3(0) #pages: 1 #objects: 6 total: 60264B seconds: 2118.533805881 SUCCESS
-----------------------------------------------------------------
```

Figura 41 Paquetes recibidos en el Servidor HTTP con Congestión. BGP-4 Escenario 4.

3.2.4.2 Escenario4: BGP-C2 en t1

En la tabla de enrutamiento que se ve en la *Figura 42*, se observa que para enviar información desde el R1 del AS1 hacia el R2 del AS2, la ruta seleccionada por el algoritmo de decisión de BGP-C2 es la ruta1, considerando como criterio de decisión la congestión presente a lo largo de la ruta (ver *Tabla 25*). El punto de salida se selecciona por medio de un valor alto del atributo LOCAL_PREFERENCE, valor que se asocia a un bajo costo de ruta, el cual se relaciona con un bajo valor de congestión y por ende a la ruta que presente una menor pérdida de paquetes.

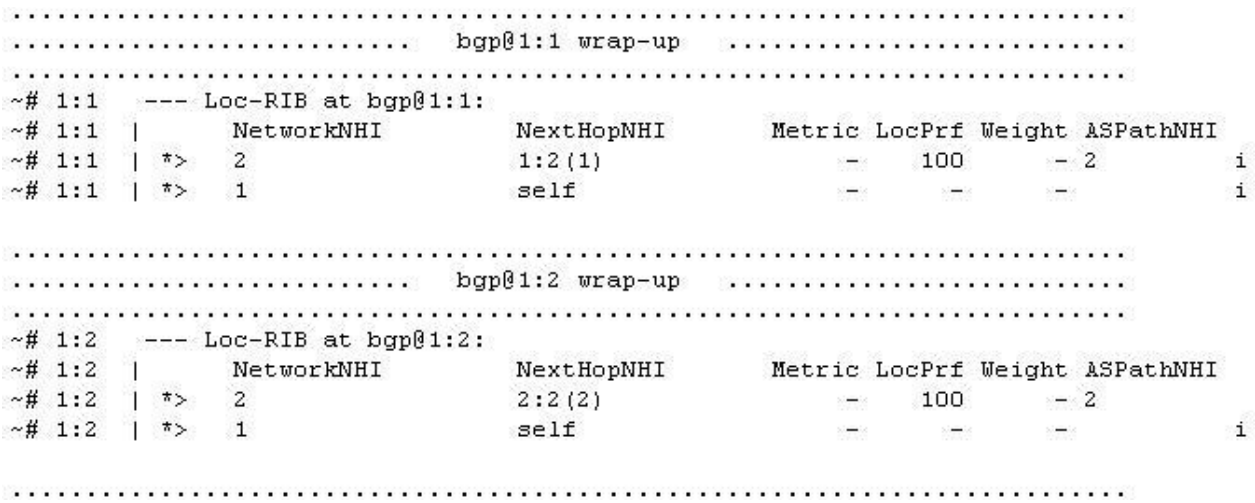

Figura 42 Tabla de Enrutamiento R1 y R2 presentes en el AS1. BGP-C2 en t1 Escenario 4.

Tabla 25 Congestión presente en cada Ruta. Escenario 4. BGP-C2 en t1

Ruta	Congestión	P. Perdidos	B. Perdidos
Ruta1	0.13	8	884.746
Ruta2	0.44	26	2.614.491

3.2.4.2.1 Grafica de Paquetes y Bytes Perdidos vs Tasa de Pérdida.

La *Tabla 26* y *Tabla 27*, muestran la cantidad de paquetes y bytes entre destino y origen. La ruta1 es la seleccionada por el algoritmo de decisión de BGP-C2 para el envío de información.

Las *Figuras 43* y *44*, representan gráficamente los datos consignados en las *Tablas 26* y *27* respectivamente.

Tabla 26 Paquetes Perdidos vs Tasa de Pérdida en la Ruta1. Escenario 4 BGP-C2

Escenario4_BGP-C2		
P. Recibidos	P. Perdidos	Tasa de Pérdida
58	0	0%
52	6	10.34%
50	8	13.79%
43	15	25.86%
38	20	34.48%

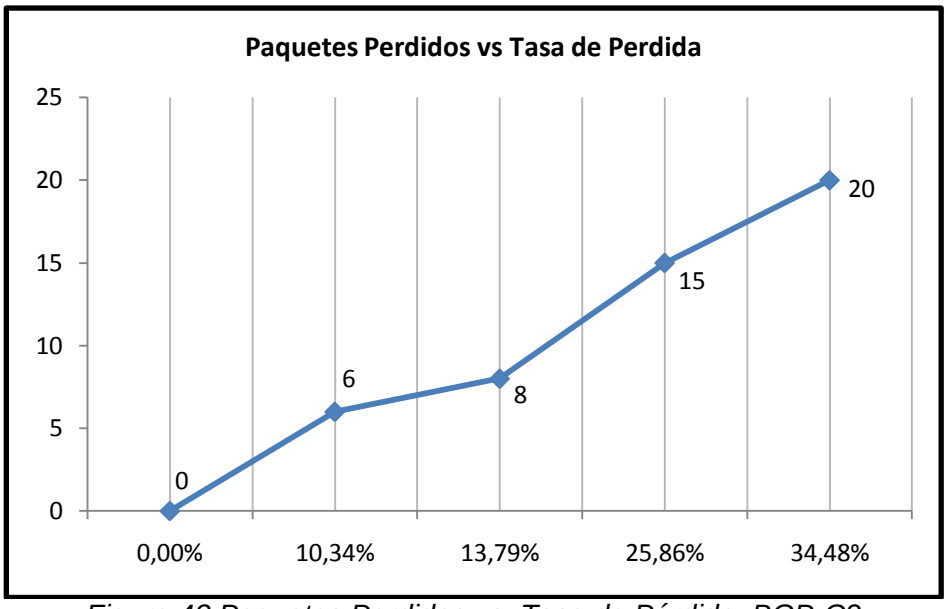

Figura 43 Paquetes Perdidos vs. Tasa de Pérdida. BGP-C2

Tabla 27 Bytes Perdidos vs Tasa de Pérdida en la Ruta1. Escenario 4 BGP-C2

Escenario4_BGP-C2		
B. Recibidos	**B. Perdidos**	**Tasa de Pérdida**
6,805,731	0	0%
6,399,397	347,632	5.11%
5,964,339	841,392	12.36%
5,360,723	1,445,008	21.23%
4,835,272	1,970,459	28.95%

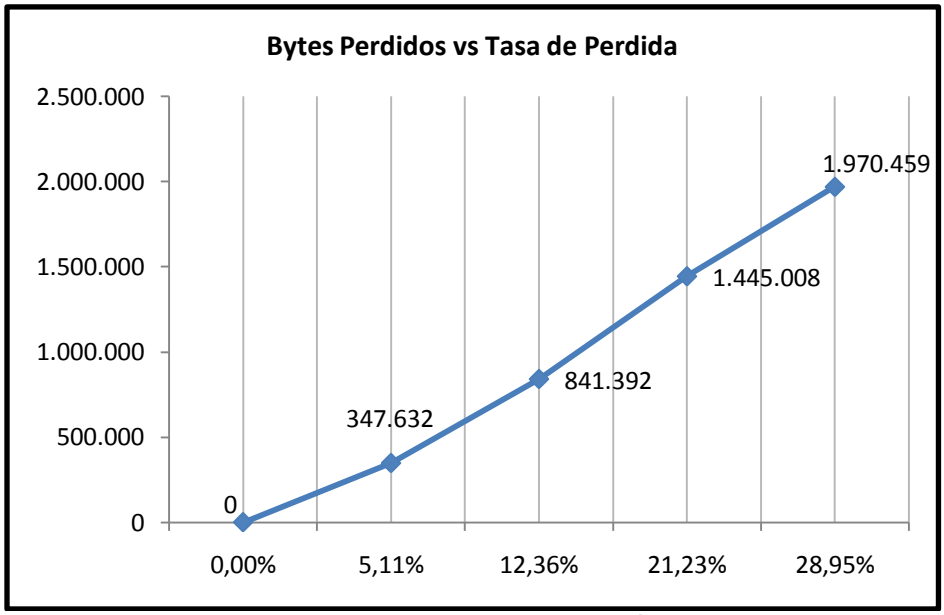

Figura 44 Bytes Perdidos vs. Tasa de Pérdida. BGP-C2

3.2.4.3 Escenario4: BGP-C2 en t2

La *Figura 45*, muestra la tabla de enrutamiento del R1 del AS1, donde se observa que la ruta2 es la seleccionada por el protocolo BGP-C2, considerando el criterio de congestión de ruta (ver *Tabla 28*). El protocolo selecciona la ruta mediante la asignación de un valor alto de LOCAL_PREFERENCE, el cual se asocia directamente a un bajo costo e inversamente al grado de congestión; este a su vez se relaciona con un bajo índice de pérdida de paquetes.

```
.....................................................................
.........................   bgp@1:1 wrap-up   .........................
.....................................................................
~# 1:1   --- Loc-RIB at bgp@1:1:
~# 1:1  |      NetworkNHI         NextHopNHI       Metric LocPrf Weight ASPathNHI
~# 1:1  | *>   2                   2:1(1)                -    100      - 2
~# 1:1  | *>   1                   self                  -      -      -           i

.....................................................................
.........................   bgp@1:2 wrap-up   .........................
.....................................................................
~# 1:2   --- Loc-RIB at bgp@1:2:
~# 1:2  |      NetworkNHI         NextHopNHI       Metric LocPrf Weight ASPathNHI
~# 1:2  | *>   2                   1:1(2)                -    100      - 2         i
~# 1:2  | *>   1                   self                  -      -      -           i

.....................................................................
```

Figura 45 Tabla de Enrutamiento R1 y R2 presentes en el AS1. BGP-C2 en t2 Escenario 4.

Tabla 28 Congestión presente en cada Ruta. Escenario 4. BGP-C2 en t2

Ruta	Congestión	P. Perdidos	B. Perdidos
Ruta1	0.33	21	501.053
Ruta2	0.05	3	2.176.159

3.2.4.3.1 Grafica de Paquetes y Bytes Perdidos vs Tasa de Pérdida.

La *Tabla 29* y *Tabla 30*, indican la cantidad de paquetes y de bytes de información perdidos en el trayecto entre el cliente HTTP y un servidor HTTP (ver *Figura 46* y *Figura 47*). La ruta2 es la seleccionada por el algoritmo de BGP-C2 para el envío de información.

Tabla 29 Paquetes Perdidos vs Tasa de Pérdida en la Ruta2. Escenario 4 BGP-C2

Escenario4_BGP-C2		
P. Recibidos	**P. Perdidos**	**Tasa de Pérdida**
58	0	0%
56	2	3.45%
49	9	15.52%
41	17	29.31%
37	21	36.21%
30	28	48.28%

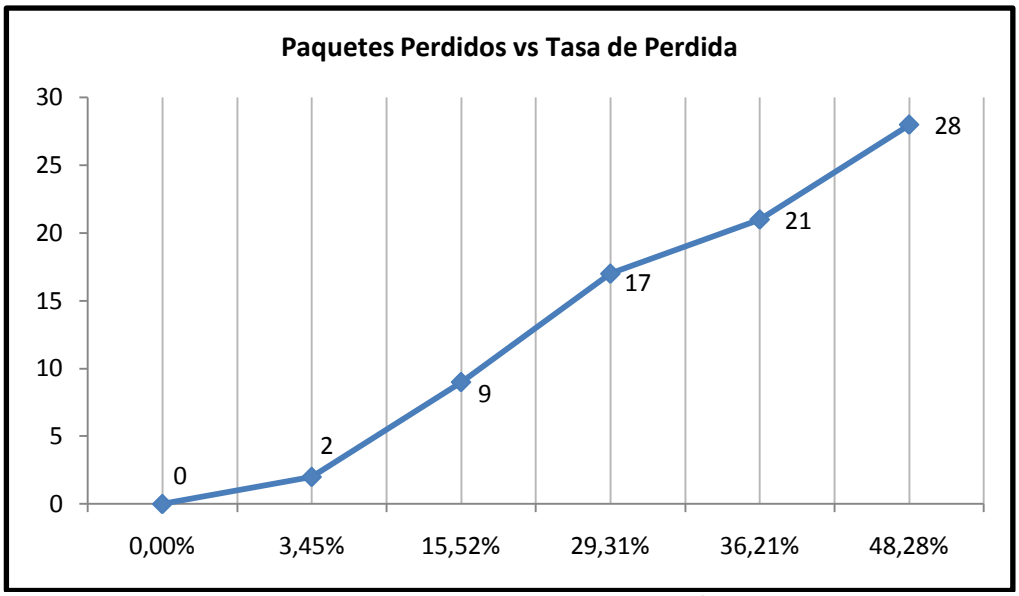

Figura 46 Paquetes Perdidos vs Tasa de Pérdida BGP-C2

Tabla 30 Bytes Perdidos vs Tasa de Pérdida en la Ruta2. Escenario 4 BGP-C2

Escenario4_BGP-C2		
B. Recibidos	**B. Perdidos**	**Tasa de Pérdida**
6,805,731	0	0%
6,510,378	295,353	4.34%
5,845,865	959,866	14.10%
5,348,913	1,456,818	21.41%
4,811,697	1,994,034	29.30%
3,946,713	2,859,018	42.01%

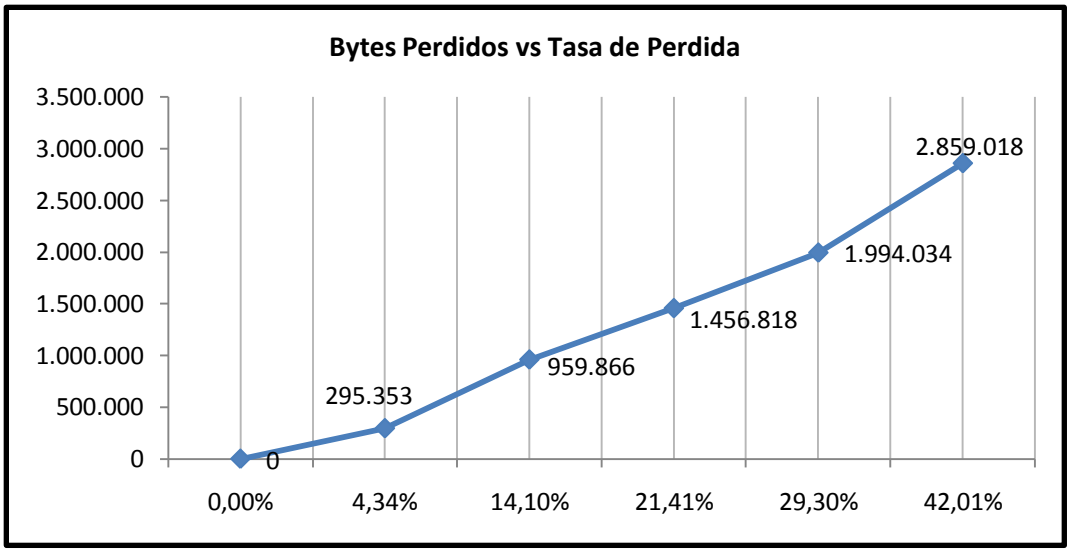

Figura 47 Bytes Perdidos vs. Tasa de Perdida. BGP-C2

El uso correcto de la de la información referenciada a lo largo de este documento fue de vital importancia para el cumplimiento total de los objetivos propuestos para generar un entorno investigativo en cuanto a la optimización del enrutamiento mediante adaptaciones del protocolo BGP-4.

Al finalizar este capítulo de Simulación, Pruebas y Resultados se observa que las topologías de red utilizadas para verificar las adaptaciones que permiten mejorar la toma de decisiones de enrutamiento considerando la congestión y la pérdida de información, fueron propicias y con complejidad suficiente, por contar con diversas características de red para el transporte de información inter-dominio; por otro lado, no inciden en los resultados esperados, debido a que el objetivo de proponer y verificar las adaptaciones del protocolo BGP-4 para mejorar la toma de decisiones de enrutamiento, en búsqueda de reducir la congestión en redes IP, se orienta al funcionamiento del algoritmo utilizado para la toma de decisiones de enrutamiento.

Por último, la herramienta de simulación SSFNet, permitió obtener resultados que muestran el buen funcionamiento de las adaptaciones del protocolo BGP-4 (BGP-C2) tanto a nivel intra-dominio como a nivel inter-dominio.

CAPITULO IV: CONCLUSIONES Y RECOMENDACIONES

A lo largo de este proyecto de grado, se genera una base conceptual profunda del funcionamiento del protocolo BGP-4 y de los inconvenientes para el enrutamiento óptimo, también una solución viable que permita superar dichos inconvenientes. Asimismo, se tuvieron en cuenta diferentes mecanismos que permiten mejorar el enrutamiento inter-dominio, considerando parámetros de red, métricas de enrutamiento y atributos propios del protocolo, para brindar en conjunto, un soporte suficiente para que BGP-C2 logre reducir la congestión en diferentes escenarios de simulación.

Lo anterior, permitió cumplir con los objetivos propuestos en este proyecto, los cuales buscan mejorar el proceso de enrutamiento con BGP-4, por medio del mejoramiento en la toma de decisiones, considerando la congestión como fenómeno que ocasiona pérdida de información. Dicha mejora, se logra adaptando el algoritmo de decisión para que tome como criterio de selección la ruta menos congestionada en lugar de considerar como primera opción aquella que presente el menor número de sistemas autónomos en el recorrido entre el origen y el destino. El protocolo con la adaptación propuesta se ha definido como BGP-C2.

Para la comprobación del correcto funcionamiento de la solución planteada, se utilizó la herramienta de simulación SSFNet, por considerarse la más idónea al ser de libre distribución y poseer características propias que fueron aprovechadas para cumplir con los objetivos propuestos, además de haber sido utilizada en un proyecto anterior enfocado a la optimización de BGP-4. Igualmente, la selección de la herramienta, permitió utilizar las topologías de red planteadas en la tesis de grado "*Estudio de Viabilidad para la Optimización de Enrutamiento IP con el Protocolo BGP*", debido a que son pertinentes con el presente proyecto de investigación, además de no incidir en los resultados esperados, por la orientación del objetivo de investigación al funcionamiento del algoritmo utilizado para la toma de decisiones de enrutamiento.

A continuación, se presentan las conclusiones para dar término a este trabajo de grado y las recomendaciones para proyectos futuros relacionados con la temática.

Respecto al trabajo mismo:

La adaptación propuesta en el presente trabajo de grado consiste en relacionar la congestión de ruta como parámetro de red, la pérdida de información como indicador y el costo de ruta como métrica de enrutamiento propia de BGP-4; dicha relación se hace de manera directamente proporcional, lo que implica que a menor congestión y menor pérdida de información, menor será el costo de la ruta, constituyéndose en una alternativa para resolver el problema de la toma de decisiones de enrutamiento.

La utilización del atributo AS_PATH, como primer criterio en el algoritmo de decisión de BGP-4, permitió identificar el gran problema que presenta el enrutamiento inter-dominio, ya que al considerar este atributo se obliga a seleccionar siempre esa misma ruta sin importar el grado de congestión y pérdida de información que se pueda generar, claro está, la misma ruta es seleccionada, siempre y cuando la topología no tenga cambios en cuanto al número de saltos presentes entre origen y destino.

La selección de la *Congestión* como parámetro de red y el *Costo* como métrica de enrutamiento, permitieron establecer un criterio de selección eficaz en el momento de asignar un LOCAL_PREFERENCE alto a la interfaz de salida de un enrutador, contribuyendo así en el mejoramiento de la toma de decisiones del proceso de enrutamiento.

La Congestión es directamente proporcional a la Pérdida de Información, lo que permite determinar y cuantificar la cantidad de información perdida de acuerdo al grado de bloqueo de una ruta.

El protocolo BGP-C2, es un conjunto de adaptaciones del protocolo BGP-4, que relaciona un parámetro de red con una métrica de enrutamiento, en la búsqueda de mejorar el proceso de la toma de decisiones, lo cual se constituye en el aporte más significativo de este trabajo de grado. Dichas adaptaciones se basaron en el estudio del comportamiento del protocolo BGP-4 definido en el RFC 4271.

Es de gran importancia contar con una herramienta software que permita realizar modificaciones al algoritmo de decisión del protocolo BGP-4 y realizar pruebas simuladas sobre escenarios establecidos, con el fin de verificar las adaptaciones de la solución propuesta.

La verificación de las adaptaciones propuestas en el presente trabajo de grado, se logró gracias al análisis del comportamiento de BGP-4, al análisis y utilización de la herramienta de simulación como software que permite la implementación de diferentes escenarios de red, así como también al estudio probabilístico para calcular la congestión presente en cada ruta. Lo anterior se constituyó en una base metodológica para obtener una serie de resultados congruentes al objetivo de este proyecto.

Respecto al mejoramiento del proceso de enrutamiento de BGP.

Los protocolos de enrutamiento juegan un papel esencial en el intercambio de información y gracias al vertiginoso avance de las redes de comunicaciones y al aumento del tráfico, éstos siempre estarán bajo la mira de los administradores de red como de los desarrolladores que buscan crear o mejorar los criterios de decisión de enrutamiento.

En este trabajo de grado, se analizó el algoritmo de decisión del protocolo BGP-4 y se propuso una alternativa para la selección de la ruta, con un criterio diferente al menor número de sistemas autónomos que se presente entre un origen y un destino, de acuerdo al menor valor de métrica que se registre; la adaptación BGP-C2, requiere conocer con antelación, la topología de la red definida mediante código DML y la congestión de una ruta para seleccionar el camino de envío.

Para mejorar la toma de decisiones de enrutamiento, es indispensable que trabajen conjuntamente variables como el parámetro de red, la métrica de enrutamiento y el atributo propio de BGP, como también las políticas administrativas.

El protocolo es utilizado por cada enrutador BGP que hace parte de la red, considerando el parámetro de red junto con la métrica de enrutamiento para realizar la selección de la ruta, evitando así contribuir con el aumento de la congestión de ese enlace, enviando los datos por una ruta menos congestionada y por tanto con menos pérdida de información.

La utilización de valores umbrales para lograr una mejor optimización es de vital importancia para evitar que se pierda una cantidad de información considerable en una trasmisión de cualquier tipo de información.

Las adaptaciones propuestas, apuntan a que no se necesite implementar mecanismos adicionales en cualquier nivel del sistema OSI, evitando así que se incurra en gastos innecesarios de equipos, infraestructura o software para realizar un enrutamiento más eficiente.

El aporte de este proyecto de grado, se basa en la adaptación del algoritmo de decisión del protocolo BGP para crear una política de selección de ruta, la cual calcula la probabilidad de congestión en todas las posibles rutas, selecciona la que presente el menor valor, ruta a la que se le asigna un menor valor de costo, el cual a su vez tiene asociado un mayor grado de preferencia representado por el atributo LOCAL_PREFERENCE.

Respecto a la simulación y a la herramienta.

Los escenarios de simulación tomados de la tesis de grado "*Estudio de Viabilidad para la Optimización de Enrutamiento IP con el Protocolo BGP*", establecidos para la verificación de la solución planteada, fueron trasparentes al objetivo de investigación y no incidieron en los resultados.

La cantidad de simulaciones realizadas a diferentes topologías de red, son necesarias y suficientes para certificar que BGP-C2 funciona correctamente según lo planteado, además permite diferenciar el proceso de decisión con respecto a BGP-4, ya que opta por la ruta menos congestionada logrando así una menor pérdida de información.

BGP-C2, además de realizar un enrutamiento inter-dominio eficiente, también puede ser utilizado en enrutamiento intra-dominio, ya que es capaz de considerar variables en los enlaces presentes dentro de su propio dominio, basando su selección en atributos del propio protocolo BGP-4.

En cada escenario analizado, se deben establecer unas condiciones iniciales de simulación que deben permanecer constantes, como el tiempo total y el tamaño en bytes de los paquetes que se envían desde un origen hacia un destino, con el fin de observar que la pérdida de información se debe a la congestión presente en una ruta, considerando que, si el tamaño del paquete varía de una ejecución a otra, no habría forma de concluir que la congestión fue la que origino la perdida de la información.

El protocolo BGP-C2, ejecuta el proceso de selección de ruta considerando la congestión más baja presente, a pesar de que estas no sean las más cortas.

SSFNet es la herramienta apropiada para el desarrollo de este proyecto de investigación, debido su libre uso y distribución, además permite hacer modificaciones al código fuente del protocolo BGP-4, lo que permite adaptarlo a las necesidades de la red.

Una falencia de SSFNet es que no trabaja en tiempo real, lo que implica que las variables asignadas manual o aleatoriamente se van a mantener durante todo el tiempo de simulación, implicando que se tenga que reconfigurar su código para una nueva simulación si se requiere, además de no poseer una interfaz grafica amable al usuario final, todas las configuraciones deben realizarse directamente en su código fuente.

RECOMENDACIONES

Explorar y difundir el uso de herramientas de simulación de software libre, sería un punto de gran beneficio tanto para la Facultad de Ingeniería Electrónica y Telecomunicaciones, como para la comunidad académica e investigativa de la Universidad del Cauca, en este caso en particular, la herramienta de simulación SSFNet fue seleccionada por ser muy completa, de uso libre, y con un gran soporte para diferentes protocolos de red.

Los escenarios de simulación utilizados en este trabajo de grado, son solo una pequeña muestra de las posibles configuraciones que se pueden encontrar en una red real, por tanto, para obtener resultados más cercanos a la realidad, y obtener un análisis ajustado a estos, es necesario recurrir a un mayor número de escenarios de simulación y si es posible, escenarios reales físicamente.

Con el objetivo de continuar con el trabajo de esta tesis, las siguientes son las propuestas para trabajos futuros:

- Estudio de la compatibilidad entre el algoritmo BGP-C2 con el mecanismo del atributo Communities privado de CISCO Systems, como complemento.

- Seleccionar otro atributo de la red como parámetro, junto con su indicador, analizando así las diferentes formas de combatir los inconvenientes de una red, al implementarse el protocolo de enrutamiento BGP-4

- Aplicación de características de TE, que contribuyan a la optimización del protocolo BGP-4, aprovechando de una mejor forma los recursos de la red.

- Buscar la posibilidad de entablar un acuerdo con CISCO Systems para la utilización de su código del mecanismo Communities, de tal forma que pueda transmitirse información de los enlaces adyacentes a cada enrutador de frontera de los AS.

- Exploración y análisis de nuevas herramientas de simulación, preferiblemente de software libre, enfocadas a la adaptación y mejoramiento de BGP-4, BGP-C2 y J2-BGP en diferentes escenarios de red.

BIBLIOGRAFIA

[1] Matthew Caesar, UC Berkeley, Jennifer Rexford, Princeton University. "BGP Routing Policies in ISP Networks".

[2] J. Gozdecki et al, "Quality of Service terminology in IP Networks," IEEE Communications Magazine, Marzo de 2003, Pág. 153-159.

[3] B. Quoitin y C. Pelsser. "*A performance evaluation of BGP-Based Traffic Engineering*", Departamento de las Ciencias de la Computación, Universidad Católica de Louvain, Bélgica. [Online]. Disponible en: http://www.info.ucl.ac.be/~bqu/downloads/ijnm-evaluation-BGP-TE.pdf [Ingreso, Junio 2009].

[4] B. Quoitin, S. Uhlig, C. Pelsser, L. Swinnen and O. Bonaventure. "*Interdomain traffic engineering with BGP*", Departamento de las Ciencias de la Computación y la Ingeniería, Universidad Católica de Louvain, Bélgica. [Online]. Disponible en: http://www.info.ucl.ac.be/~obo/papers/commag-may2003.pdf [Ingreso, Abril 2009].

[5] S. Halabi y D. McPherson. "*Internet Routing Architectures",* Segunda Edición. Cisco Press. ISBN: 1-57870-233-X, Agosto 2003.

[6] T. Erlebach, "*Autonomous Systems in the Internet: A Potential Subject for Studying Self-* Aspects".* Disponible en: http://www.cs.unibo.it/self-star/papers/erlebach.pdf.

[7] IANA (2007). IANA. Internet Assigned Numbers Authority. [Online] Disponible en: http://www.iana.org/assignments/as-numbers. [Ingreso, Mayo 2009].

[8] "*Enrutamiento por Internet*." *Kioskea.net*, Octubre, 2008. [Online]. Disponible en: http://es.kioskea.net/contents/internet/routage.php3 [Ingreso, Mayo. 2009].

[9] S. M. Ballew. "*Managing IP Networks with Cisco Routers"*. Primera Edición. Octubre 1997. Disponible en: http://oreilly.com/catalog/cisco/chapter/ch05.html.

[10] J. Diez, "*Enrutamiento y Protocolos de Enrutamiento*", Universidad de la Rioja. Logroño, España. Abril, 2008. [Online]. Disponible en: https://belenus.unirioja.es/~judiez/trabajoarssi/p2c.html [Ingreso, Mayo. 2009].

[11] B. Quoitin, "*BGP-based Interdomain Traffic Engineering*", Facultad de Ciencias Aplicadas, Departamento de Ingeniería Informática, Universidad Católica de Louvain, Bélgica. Agosto 2006

[12] E. Collado, "*Fundamentos De Routing*", Ed. 2. ISBN: 978-1-4092-8463-5. Mayo, 2009. [Online]. Disponible en: http://www.eduangi.com/node105.html [Ingreso, Junio 2009].

[13] E. Anguiano. "*Enrutamiento Dinámico RIP, OSPF, BGP*", Escuela Politécnica Superior, Madrid, España. [Online]. Disponible en: http://afrodita.unicauca.edu.co/~mtrujillo/tesis.swf [Ingreso, Junio. 2009].

[14] "*Algoritmos De Enrutamiento*", Universidad Blas Pascal, Córdoba, Argentina. [Online]. Disponible en: http://mi.ubp.edu.ar/archivosmiubp/MaterialDeEstudio/13/R-II/1497/algor_enrut.pdf [Ingreso, Junio 2009].

[15] C. Huitema, "*Routing in the Internet*", Books Craft, Indianapolis.1999.

[16] "*History of the Internet*", *historyofthings.com*, 2009. [Online]. Disponible en: http://www.historyofthings.com/history-of-the-internet [Ingreso, Junio. 2009].

[17] Y. Rekhter, T. Li, y S. Hares. "A Border Gateway Protocol 4 (BGP-4)", Internet Society RFC4271. IETF. Enero 2006. [Online]. Disponible en: http://www.ietf.org/rfc/rfc4271.txt [Ingreso, Abril. 2009].

[18] W. Stallings, "*Comunicaciones Y Redes De Computadores",* Séptima Edición. Pearson Educación. ISBN: 8420541109. 2004.

[19] O. Gerometta, "Introducción a BGP-4", *librosnetworking.blogspot.com*, Noviembre, 2006. [Online] Disponible en: http://librosnetworking.blogspot.com/2006/11/introduccin-bgp4.html. [Ingreso, Abril 2009].

[20] "*Protocolos Exteriores de Encaminamiento (BGP)*". Departamento de Sistemas Telemáticos y Computación. Universidad Rey Juan Carlos. Madrid. Mayo de 2009. [Online]. Disponible en: http://gsyc.escet.urjc.es/moodle/file.php/17/Curso_2008_2009/Teoria/7-encaminamiento-EGP-BGP.pdf [Ingreso, Marzo 2009].

[21] S. Barajas. "*Seguridad en BGP*". Doctorado en Tecnologías de las Comunicaciones, Universidad Carlos III, Madrid, España. [Online]: Disponible en: http://www.saulo.net/pub/inv/BGP-art.htm [Ingreso, Abril 2009].

[22] Cisco Systems, "*How BGP Routers Use the Multi-Exit Discriminator for Best Path*". Cisco Systems. Septiembre 2004.

[23] "*Router Teldat, Interfaz LoopBack*", Universidad Carlos III de Madrid, Departamento de Ingeniería Telemática, Madrid, España. [Online]. Disponible en: http://www.it.uc3m.es/~teldat/TeldatC/castellano/interfaces/Dm743v10_Interfaz_loopback.PDF [Ingreso, Junio 2009].

[24] A. Delfino, S. Rivero y M. San Martin, "*Ingeniería de Tráfico en Redes MPLS*." Universidad de la República, Uruguay. [Online]. Disponible en: http://telcom2006.fing.edu.uy/trabajos/mvdtelcom-002.pdf [Ingreso, Abril 2009].

[25] D. Awduche, A. Chiu, A. Elwalid, I. Widjaja y X. Xiao, "*Overview and Principles of Internet Traffic Engineering*", Internet Society RFC3272, Mayo, 2002. http://www.faqs.org/rfcs/rfc3272.html.

[26] B. Fortz, J. Rexford y M. Thorup, "*Traffic Engineering With Traditional IP Routing Protocols*." Universidad Católica de Louvain, Bélgica y AT&T Labs-Research. [Online]. Disponible en: http://www.cs.princeton.edu/~jrex/papers/ieeecomm02.pdf [Ingreso, Mayo. 2009].

[27] S. Uhlig y B. Quoitin, "*Tweak-it: BGP-based Interdomain Traffic Engineering for transit ASs*", Departamento de las Ciencias de la Computacion y de la Ingeniería. Universidad Católica de Louvain, Bélgica. Octubre 2005. [Online]. Disponible en: http://totem.info.ucl.ac.be/publications/papers-elec-versions/NGI05_Uhlig.pdf] [Ingreso, Feb. 2009].

[28] D. Buschiazzo, "*Ingeniería de Tráfico y MPLS*", Universidad de la República, Uruguay. [Online]. Disponible en: http://iie.fing.edu.uy/ense/asign/telef/mpls_te.pdf [Ingreso, Mayo. 2009].

[29] W. Muñoz y M. Trujillo. "*Mecanismos de Balanceo de Carga en MPLS Con RSVP-TE y OSPF*." Presentación de tesis, Universidad Del Cauca. 2006. [Online]. Disponible en: http://afrodita.unicauca.edu.co/~mtrujillo/tesis.swf [Ingreso, Abril 2009].

[30] Y. Ossama y S. Fahmy, "*Constraint-Based Routing in the Internet: Basic Principles and Recent Research*", Departamento de las Ciencias de la Computación, Purdue University, E.U. [Online]. Disponible en: http://www.cs.purdue.edu/homes/fahmy/papers/routing.pdf [Ingreso, Junio 2009].

[31] B. Quoitin y C. Pelsser. "*A performance evaluation of BGP-Based Traffic Engineering*", Departamento de las Ciencias de la Computación, Universidad Católica de Louvain, Bélgica. [Online]. Disponible en: http://www.info.ucl.ac.be/~bqu/downloads/ijnm-evaluation-BGP-TE.pdf [Ingreso, Junio 2009].

[32] A.S. Tanenbaum, *Computer Networks*. Prentice-Hall, 1996.

[33] D.K. Saikia y M. Dahal, "*Packet Loss Free Congestion Control in TCP for Controlled Packet Latency and Optimal Throughput*", Departamento de Ciencias de la Computación, Universidad de Tezpur y Centro Nacional de Informatica, Sikim, India. [Online]. Disponible en: http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1273336 [Ingreso, Octubre 2009].

[34] N.K.G. Samaraweera, "*Non-congestion Packet Loss Detection for TCP Error Recovery Using Wireless Links*", Departamento de Ingeniería, Universidad Aberdeen. Escocia. [Online]. Disponible en: http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=803782 [Ingreso, Octubre 2009]

[35] CCNA Exploration 4.0. "*Introducción al enrutamiento dinámico*", Capitulo 3. Disponible en: http://tech-freaks.net/wp-content/uploads/CCNA4.0-Capitulo03.pdf [Ingreso, Junio 2009].

[36] Nick Feamster Jay Borkenhagen Jennifer Rexford. "*Guidelines for Interdomain Trafic Engineering*", Laboratory for Computer Science, AT&T IP Services e Internet and Networking Systems. Disponible en: http://www.cc.gatech.edu/~feamster/publications/ccr2003-bgpte.pdf.

[37] O. Bonaventure y B. Donnet. "*On BGP Communities*", Universidad Católica de Louvain, Departamento de las Ciencias de la Computación y la Ingeniería, Universidad Católica de Louvain, Bélgica. [Online]. Disponible en: http://portal.acm.org/citation.cfm?id=1355743.

[38] T. C. Bressoud. "*Optimal Configuration for BGP Route Selection*", University Granville, Ohio Intel Research Pittsburgh Pittsburgh, Rajeev Rastogi Mark A. Smith Lucent Technologies Bell Labs.

[39] "*Norma Técnica del Servicio de Valor Agregado de Acceso a Internet.*" Consejo Nacional de Telecomunicaciones, CONATEL. Octubre, 2006. Quito, Ecuador. [Online]: Disponible en: *157.100.3.63/pdf/norma.pdf* [Ingreso, Octubre 2009]

[40] G. Velasco y P. Marian. Probabilidad y estadística para ingeniería y Ciencias. México. Thomson Editores, 2005.

[41] "Como Citar Referencias". *IEEE Style*, Julio, 2008. [Online]. Disponible en: ftp://ftp.unicauca.edu.co/Facultades/FIET/IPET/IEEE-Style.pdf [Ingreso, Noviembre. 2008].