Universidad Politécnica de Madrid
Escuela Técnica Superior de Ingenieros de Telecomunicación

DISEÑO DE PRÁCTICAS DE ENCAMINAMIENTO BGP EN REDES VIRTUALES

TRABAJO FIN DE MÁSTER

Adolfo Exebio Poumian

2013

Universidad Politécnica de Madrid
Escuela Técnica Superior de Ingenieros de Telecomunicación

Máster Universitario en
Ingeniería de Redes y Servicios Telemáticos

TRABAJO FIN DE MÁSTER

DISEÑO DE PRÁCTICAS DE ENCAMINAMIENTO BGP EN REDES VIRTUALES

Autor
Adolfo Exebio Poumian

Director
Luis Bellido Triana

Departamento de Ingeniería de Sistemas Telemáticos

2013

Resumen

Las redes de comunicaciones se han diseñado con el fin de lograr la transmisión de información mediante el intercambio de datos entre ellas, estas constan de diferentes arquitecturas y diseños para alcanzar este objetivo. Hoy en día las comunicaciones constan de diferentes protocolos dependiendo del tipo de tecnología que se este utilizando, el medio y la capa con en la que se este realizando la transmisión de información.

La convergencia de las diferentes redes de comunicaciones que existen en el mundo como Telecomunicaciones, televisión, radio, satélite, etc, conlleva a un crecimiento tanto tecnológico como para la sociedad ya que la gama de servicios que se pueden ofrecer por medio de esta convergencia es muy amplia. Al tener todas estas tecnologías acopladas se ha creado un intercambio de información masivo con cantidades de datos muy fuertes; es por eso que existe la necesidad de tener protocolos dentro de la red para controlar tal intercambio y poder ofrecer una comunicación eficaz y eficiente.

Internet en la actualidad es el factor mas importante que existe para que esta convergencia haya tenido lugar ya que la suite de protocolos que utiliza ha sido estandarizada para casi cualquier servicio y esta suite esta compuesta principalmente por los protocolos IP y TCP. Las redes IP se basan en la tecnología de conmutación de paquetes para ofrecer una comunicación mas confiable ya que de esta manera se reduce la perdida de comunicación por caídas de enlaces o desconexiones. Hoy en día en el Internet para desplegar la cantidad de información que generan las personas en el mundo se necesita tener control y poder administrar la inmensa lista de direcciones IP y rutas que se anuncian para poder lograr la comunicación.

En este documento se abordara el protocolo BGP el cual es utilizado para intercambiar información en el internet y la robusta cantidad de datos que se maneja. En la primera sección este documento se analiza el estado del arte del protocolo BGP comprendiendo las características mas importantes y el tipo de configuración que se necesita aplicar para obtener comunicación entre redes por medio del mismo. En la segunda sección se implementa una red diseñada con las ventajas y algunas características que ofrece BGP para el control del trafico; para su desarrollo se han utilizado herramientas de simulación de escenarios de trafico de red y virtualización de maquinas. Y por ultimo en la tercera sección se presentan una propuesta de ejercicios para el alumnado de grado de la Universidad Politécnica de Madrid para que con la red implementada se obtenga un estudio y una mejor compresión del protocolo desde el punto teórico y practico.

Abstract

Communication networks have been designed with to achieve the transmission of information through the exchange of data between them, these consist of different architectures and designs to achieve this goal. Today communications consist of different protocols depending on the type of technology they are using, the medium and the layer in which is performed the transmission of information.

The convergence of the different communications networks that exist in the world as telecommunications, television, radio, satellite, etc., leads to a growth of both technology and society because the range of services that can be offered by this convergence is very wide. By having all of these technologies coupled has created a massive information Exchange with incredibles amounts of data, which is why there is the need for in-network protocols to control such exchange and to offer an effective and efficient communication.

Internet today is the most important factor that exists for this convergence has taken place since the suite of protocols that uses have been standardized in almost any service, and this suite is composed mainly of IP and TCP protocols. IP networks are based on packet switching technology to provide a more reliable communication since this will reduce the loss of communication connections or disconnections falls. Today on the Internet to display the amount of information generated by people in the world need to control and manage the vast list of IP addresses and routes that are advertised in order to achieve communication.

This paper will see BGP protocol which is used for exchanging information in the internet and the robust amount of data that is handled. In the first section of this paper discusses the state of the art BGP comprising the most important characteristics and the type of configuration that needs to be applied for communication between networks using the same. In the second section implements a network designed with the advantages and some features offered BGP traffic control, for developing simulation tools have been used for network traffic scenarios and virtualization of machines. And finally in the third section presents a proposal of exercises for undergraduate students at the University Politecnica de Madrid for the deployed network to obtain a better understanding and study fo theprotocol from theoretical and practical point.

Índice general

Table of Contents

Índice de figuras

Índice de tablas

Siglas

AS: Autonomous System

BGP: Border Gateway Protocol

eBGP: Exterior Gateway Protocol

EGP: Exterior Gateway Protocol

IANA: Assigned Number Authority

iBGP: Interior Border Gateway Protocol

IGP: Interior Gateway Protocol

ISP: Internet Service Provider

IP: Internet Protocol

LAN: Local Area Network

MED: Multi Exit Discriminator

RIR: Registros Regionales de Internet

TCP: Transport Control Protocol

VNX: Virtual Networks over LinuX

1. Introducción

1.1 Contexto

La mayor red existente en el globo terráqueo es el Internet, ya que es la interconexión de todas las redes de comunicaciones la cual es utilizada para la distribución de información. En el transcurso del tiempo el Internet ha tenido un crecimiento explosivo, esto conlleva a que dentro de ella viaja una gran cantidad de información generada todos los días por los usuarios los cuales buscan conectarse a la red para el intercambio de información y búsqueda de la misma, es por eso que también IPv4 se vio en la necesidad de evolucionar a IPv6 ya que el rango de direcciones con el que se contaba no era necesario para soportar este crecimiento y en algún momento se terminarían; al tener este tipo de crecimiento, tales cantidades de información y direcciones IP se tiene la necesidad de administrar y controlar de manera eficaz y eficiente esta red, por lo que para llegar a tener este tipo de administración se deben implementar protocolos los cuales permitan controlar y administrar la información y las grandes tablas de rutas que alberga el Internet. El protocolo de enrutamiento que proporciona accesibilidad y la ruta de la Internet es el Border Gateway Protocol (BGP). BGP es definido por RFC 1771 protocolo de red como sistema de inter-Autónoma de enrutamiento utilizada para intercambiar información con otros sistemas conocidos como BGP Sistemas Autónomos (AS), este protocolo proporciona un sistema libre de bucles de enrutamiento Entre Entre AS y otros dominios. Debemos recordar que un AS es un conjunto de routers bajo una administración única, por lo que los routers de un AS puede utilizar múltiples Protocolos de Gateway Interior (IGP) para intercambiar información de enrutamiento dentro del AS y un Protocolo de Gateway Exterior para enrutar al exterior. Una diferencia entre BGP y el IGP es que BGP tiene un Algoritmo de selección de ruta mas robusto. Este algoritmo se utiliza para elegir la mejor ruta BGP con reglas más complejas llamadas Atributos BGP. Con este protocolo se puede obtener una visión completa de la topología de red con cada AS interconectado, y facilitar el identificar bucles en al red y eliminarlos.

1.2 Objetivos

El propósito de este documento es el estudio, comprensión e implementación del protocolo BGP, por lo que se han establecido los siguientes objetivos.

1. Realizar un estudio teórico del protocolo BGP para identificar sus capacidades, aplicaciones y ventajas
2. Desarrollar una red de datos en la cual implemente el protocolo BGP para visualizar de mejor manera sus funciones, operación y comportamiento.
3. Trasladar el conocimiento teórico y practico al alumnado de la carrera de Telecomunicaciones de la Universidad Politécnica de Madrid elaborando ejercicios de configuración y análisis sobre la red implementada con el protocolo BGP

1.3 Metodología

Para realización del apartado de investigación de la tecnología se hizo uso de la bibliografía ofrecida por la biblioteca de la escuela de Telecomunicaciones de la Universidad Politécnica de Madrid las cuales de las cuales se obtuvo la parte teórica y casos prácticos para comprender de mejor manera la configuración a implementar y obtener elaborar un diseño de red de acuerdo al estudio realizado. En la parte de implementación de red se abordo por medio de documentación, plataformas y softwares desarrollados y ofrecidos por la misma escuela de Telecomunicaciones, estudiando dicha documentación para comprender el funcionamiento de las plataformas y así de esta manera poder implementar la red deseada por medio de la virtualización de maquinas.

Finalmente el apartado de ejercicios de docencia fue estructurado en base a ejercicios basados en otros protocolos de ruteos los cuales son utilizados en la actualidad para impartir clase en la universidad. Los ejercicios fueron adaptados al formato actual para no perder la línea de trabajo ya implementada.

1.4 Estructura de la memoria

Una vez dada la introducción y que hayan quedado claros los objetivos que contiene el primer capitulo se procederá a los siguientes capítulos los cuales abordan el tema con mayor precisión.

El segundo capitulo contiene un estudio completo el cual describe las capacidades, características, ventajas y parámetros de configuración del protocolo BGP.

Los Capítulos tercero, cuarto y quinto describen la red implementada por medio de software de virtualización, demonios para emular equipos de datos; contiene las características de BGP que fueron implementadas y los resultados obtenidos de la implementación con sus respectivas pruebas.

El documento finalizara en el sexto capitulo el cual se dedico a la realización de ejercicios sobre la red implementada para que el conocimiento aprendido tanto teórico como practico sea trasladado a los alumnos de la carrera de Telecomunicaciones de la Universidad Politécnica de Madrid.

2. Fundamentos de teoría

2.1 Organización de Internet

2.1.1 Proveedores de Servicio de Internet (ISP)

BGP al ser el protocolo utilizado para el intercambio de rutas en Internet es utilizado por los ISP para interconectarse entre ellos, así de esta manera también se ellos pueden ofrecer interconexión con clientes en cualquier parte del mundo. Los ISPs están clasificados en Tier 1, Tier 2 y Tier 3, esta clasificación depende de su alcance geográfico, es decir el tamaño de infraestructura que poseen para ofrecer su servicio, por lo tanto algunos ISP tienen que pagar a otros ISPs para que transporten su trafico o transito y algunos ISP de gran tamaño se interconectan con otros ISP del mismo tamaño para intercambiar trafico, pero no hay ganancia monetaria, solo intercambio de trafico del cual beneficia a los dos. A continuación se detallara un poco mas la diferencia entre cada Tier.

2.1.2 Clasificación de Tier

- Tier 1: Estos ISPs son tan grandes que no pagan a ningún ISP por tránsito, esto es por que se conectan con otros ISPs del mismo tamaño, de esta manera se logra obtener conectividad en todo el internet (todas las demás redes tienen que pagar al menos a algún Tier 1 por transito) [1] .

- Tier 2: Estos ISPs poseen una red de gran tamaño, pero no lo suficiente como para intercambiar trafico con los Tier 1 y convencerlos de conectarse con ellos, así que al menos tienen que conectarse con algún Tier1 y pagar por transito [1] .

- Tier 3:Este tipo de ISP son pequeños y generalmente operan de manera local así por lo tanto deben conectarse a uno o varios Tier 1 Tier 2 [1] .

2.1.3 Sistemas Autónomos (ASes)

Un AS es un conjunto de redes IP el cual esta definido por políticas de encaminamientos propias, totalmente independiente de los AS diferentes. BGP se basa en AS de manera que para conectarse entre AS es por medio del protocolo BGP. El uso de ASes facilita el intercambio de información de encaminamiento ya que los ISPs no se tienen que preocupar por la red interna de los demás ISPs sino que los ven como un solo dominio de administración y así se puede aligerar las tablas de encaminamiento que se manejan en el internet y se crea una lista de ASes por la cual viaja la información de encaminamiento. Estos Sistemas Autónomos son gestionados y asignados por diferentes entidades como Internet Asigned Numbers Authority (IANA) y Registros Regionales de Internet (RIR) [1] .

2.2 Protocolo BGP (Border Gateway Protocol)

BGP esta clasificado como un protocolo de borde, el cual es utilizado para el intercambio de información de encaminamiento entre ASes, a diferencia de los demás protocolos esta implementado como protocolo de Vector de Rutas (Path Vector) tomando cada AS como un único punto en la ruta para algún destino en lugar de tomar cada router como un único punto. Al operar con ASes la manera de anunciar los prefijos entre ASes lo hace por medio de una lista que contiene los prefijos a anunciar y los ASes necesarios para alcanzar el prefijo, esta lista se llama *AS Path*, esta misma manera de operar es la que se utiliza para prevenir los bucles, ya que en caso de recibir

una ruta con el numero de AS que esta instalado localmente esta será rechazada, un ruta BGP es una asociación de la ruta con ciertos atributos para llegar a ese destino. Algo inusual es que BGP protocolo funciona sobre TCP en el puerto 179, esto es para utilizar las características del protocolo TCP, enfocarse en procesar la información de encaminamiento y enviar broadcast y unicast para descubrir vecinos [1] . Cuando se establece una sesión TCP entre vecinos comienza un intercambio de información en forma de mensajes tales como Open, Update, Notification y Keepalive dentro de una sesión BGP hay más tipos de mensajes como negociación de parámetros, pero estos son los más importantes en una sesión BGP estos mensajes se detallaran mas adelante.

BGP trabaja sobre dos tipos de enlaces, los cuales están divididos en Enlaces Internos y Enlaces Externos, de manera que sesiones BGP entre enlaces dentro de el mismo AS se denominas sesiones internas BGP (iBGP) y las sesiones BGP creadas entre enlaces pertenecientes a diferentes ASes son denominadas sesiones externas BGP (eBGP). La principal diferencia entre este tipo de enlaces son las siguientes:

- Las rutas aprendidas entre enlaces iBGP no son anunciadas a sus otros enlaces iBGP
- Los atributos de ruta aprendidos en una sesión iBGP generalmente no impacta en la decisión para alcanzar una ruta que esta en el exterior
- El atributo AS Path no cambia entre enlaces iBGP, el AS local solo es agregado en la ruta cuando se quiere anunciar al exterior por medio de un enlace eBGP
- El atributo Next Hop no cambia cuando se anuncia ruta a un enlace iBGP, este solo cambia cuando la ruta es anunciada a un enlace eBGP poniendo la dirección IP local del router que esta anunciando la ruta

2.2.1 Mensajes BGP

Los mensajes BGP son utilizados para anunciar información de encaminamiento nueva, retirar las rutas previamente anunciadas o ambos. La información que se anuncia por medio de BGP es un conjunto de rutas o prefijos asociados a atributos BGP [1] .

- Open: Este tipo de mensaje es utilizado por BGP para establecer una sesión BGP una vez que la conexión TCP se establece

- Update: Esta es una de las más importantes de BGP, porque estos mensajes informó el anuncio de prefijos nuevos, estos mensajes se generan cada vez que un enrutador calcula una mejor ruta a un destino

- Notification: Estos mensajes son utilizados por BGP para informar de errores y cerrar una sesión BGP

- Keepalive: Estos mensajes son utilizados por BGP para controlar el equipo con el que se creó una sesión BGP y verificar que está vivo y activo

2.2.2 Estados BGP

BGP tiene diferentes estados con los que podemos identificar el comportamiento que presenta el router en el momento que se lleva acabo el proceso de sesión de BGP, los estados que puede tener BGP son [1] :

- Idle: El router está esperando un evento inicial, como enable BGP, la inserción de un vecino con el cual se levantara una sesión BGP o que una interfaz se active

- Connect: El router espera a que se complete su propia sesión TCP para escuchar las sesiones TCP entrantes

- Active: BGP espera para una sesión TCP

- OpenSet: El mensaje Open fue enviado pero el router sigue esperando la respuesta del equipo con el que está tratando de crear una sesión BGP

- OpenConfirm: El mensaje de respuesta ante el mensaje Open previamente enviado fue recibido, pero aún no ha recibido ningún mensaje KeepAlive

- Established: El router ha recibido el primer KeepAlive y ahora la transmisión de mensajes de Update, Notification y KeepAlive puede comenzar

2.2.3 Método de Selección de Ruta utilizado por BGP

La mayoría de las redes BGP conectan con varias redes a su vez, esto es para tener mas de una ruta disponible para los prefijos anunciados en la red, de manera que una vez establecida una sesión BGP el router empieza a intercambiar información de encaminamiento con sus vecinos BGP, al recibir esta información BGP realiza la selección y almacenamiento de las rutas mas optimas para el encaminamiento, de manera que primero son insertadas todas las rutas en la tabla de BGP, se comparan todas las rutas por medio el *Algoritmo de Selección de Ruta BGP* el cual para dicha selección utiliza *Atributos BGP,* se elige la ruta mas optimas para todos los prefijos, posteriormente se instala en la tabla de encaminamiento y se advierten las rutas con los vecinos BGP [1] .

2.2.4 El algoritmo de selección de ruta

Este es el algoritmo que utiliza BGP para la selección de ruta a través de los Atributos BGP, a continuación se muestra la secuencia que sigue para evaluar las rutas BGP a través de los Atributos [1] :

- WEIGHT Mayor
- LOCAL PREFERENCE Mayor
- LOCALLY ORIGINATED
- AS-PATH
- ORIGIN Minor (IGP <EGP <incomplete)
- LowMED

2.2.5 Inicializando BGP

BGP se basa en Sistemas Autónomos para definir las comunicaciones entre dos routers que se encuentran ya sea en el mismo o en Sistemas Autónomos diferentes, es por eso que al habilitar BGP tiene que estar asociado con un AS y así creada la instancia de BGP se puede comenzar a establecer vecinos BGP con sus respectivos sistemas autónomos y así crear vecindades entre equipos y declarar que se desea anunciar rutas a través de BGP. Los comandos de configuración se presentan a continuación [1] .

- *router bgp <AS number> (Activa BGP)*
- *network <network address> mask <mask> (Prefijo a ser anunciado)*
- *neighbor <ip address> remote-as (Dirección y AS del vecino)*

En la Figura 1 se muestra la combinación de la configuración previamente mencionada con valores para su mejor entendimiento

```
!
Router bgp 60055
 network 192.0.2.0 mask 255.255.255.0
 neighbor 192.0.254.17 remote-as 40077
 neighbor 192.0.254.17 description BGP session to ISP A
!
```

Figura 1: Configuración básica BGP [1]

En esta configuración el router crea una instancia BGP para su AS 60066, posteriormente con el comando Network se anuncia la red 192.0.2.0 con una determinada mascara, con los comandos Neighbor se crea una vecindad BGP con el vecino 192.0.254.17 el cual tiene un numero de AS 40077 y finalmente se le da una descripción para identificar el enlace que se esta creando.

2.2.6 Instancias BGP

BGP tiene dos variantes, BGP Interno y BGP Externo en configuración son muy similares, la diferencia en la configuración marca el límite entre zonas de conexión perteneciente mismos Sistemas Autónomos o diferentes.

2.2.7 BGP Interno (iBGP)

BGP Interno se utiliza dentro de un AS cuando dos o más enrutador quiere comunicarse entre sí a través de BGP, así de esta manera se obtiene una imagen completa de la red y también se puede determinar qué router es el punto de conexión con otro AS como un ejemplo Internet Proveedor de servicios [1] .

A continuación se muestra en la Figura 2 la configuración de un router mediante iBGP. Nótese que al declarar la vecindad con el vecino se utiliza el mismo número de AS que la instancia del mismo router, de esta manera se declara que los equipos hablan BGP de manera interna ya que están dentro del mismo AS. El comando *next-hop-self* se utiliza para declarar y de alguna manera forzar que el vecino se vea en la tabla BGP como el siguiente salto.

```
!
hostname BR1
!
interface Ethernet1
 ip address 192.0.2.49 255.255.255.252
 description Connection to BR2
!
router bgp 60055
 no synchronization
 neighbor 192.0.2.50 remote-as 60055
 neighbor 192.0.2.50 description iBGP session to BR2
 neighbor 192.0.2.50 next-hop-self
!
```

Figura 2: Configuración iBGP [1]

2.2.8 BGP Externo eBGP

BGP Externo se utiliza para enviar y recibir información entre sistemas BGP pero que están en diferentes Sistemas Autónomos.

La Figura 3 muestra la configuración de eBGP en el que estamos creando la instancia BGP con el AS 60055, posteriormente se crea una vecindad con el equipo 219.2.19.1 que está asociada a AS 50066. Fue introducido la configuración iBGP Previos para ver la diferencia entre ellos y ver qué vecino usa iBGP y cuales eBGP.

```
 hostname BR2
!
interface Ethernet1
 ip address 192.0.2.50 255.255.255.252
 description Connection to BR1
 no ip directed-broadcast
!
interface Serial0
 description ISP B
 encapsulation ppp
 ip address 219.2.19.2 255.255.255.252
!
router bgp 60055
 network 192.0.2.0
 neighbor 192.0.2.49 remote-as 60055
 neighbor 192.0.2.49 description iBGP session to BR1
 neighbor 192.0.2.49 next-hop-self
 neighbor 219.2.19.1 remote-as 50066
 neighbor 219.2.19.1 description BGP session to ISP B
 neighbor 219.2.19.1 filter-list 1 in
 neighbor 219.2.19.1 filter-list 2 out
 neighbor 219.2.19.1 distribute-list 3 out
!
```

Figura 3: Configuración eBGP [1]

2.3 Ingeniería de Trafico

Ingeniería de tráfico es una de las características que tenemos con BGP como la mejor opción para elección de enlaces en caso de que haya que conectar con dos proveedores diferentes.

Cuando hablamos de Ingeniería de trafico para la elección de los enlaces por el cual queremos que viaje el trafico no necesariamente se tiene que hacer una decisión basada en el Ancho de Banda, Retraso y Perdida de Paquetes, ya que muchas veces el mejor enlace a escoger no es el que tiene mayor ancho de banda, sino se puede elegir un enlace de acuerdo a la carga que presenta, fiabilidad, etc [1] . Con BGP se puede realizar ingeniería de trafico manipulando el trafico basándose en la modificación de los Atributos BGP, también se puede hacer balanceo de trafico para así explotar de mejor manera los enlaces.

4.1 Mapas de Ruta

Los Mapas de Ruta es una de las herramientas mas utilizadas por BGP para crear políticas de encaminamiento, ya que con esta herramienta se pueden modificar los atributos como *Local preference, AS-path, MED, Comunidades* y Weight para influir en la selección de la ruta y la forma en que BGP añade las rutas a su tabla, cabe mencionar que esta herramienta también puede ser utilizada con Prefix-list y listas de acceso [1] .

El modo de operación es simple, ya que es una serie de declaraciones para comprobar si una ruta coincide con la política creada y asi aceptar rutas, denegar rutas o modificar atributos. Utilizando la línea de comando de "*match*" se crea una combinación utilizando los parámetros *as-path, community, ip address, ip next-hop y metric*, posteriormente se aplica la line a de comando "*set*" con los parámetros *local-preference, as-path, community, ip address, ip next-hop, weight* y *metric* para realizar su modificación. Los Mapas de Ruta también se les asignan etiquetas y llevan una secuencia para realizar su proceso [1] .

4.2 Atributos BGP

Los Atributos BGP es información utilizada por el protocolo BGP para dar o identificar preferencia en las rutas anunciadas entre los enlaces BGP, estos son utilizados dentro o fuera de un AS. Los Atributos los podemos clasificar de acuerdo a la manera en la que influyen de la siguiente manera [4]:

- Atributos bien conocidos y obligatorios: Atributos que son reconocidos por todos los routers BGP y están incluidos en todas las actualizaciones
- Atributos bien conocidos y direccionales: Atributos que son reconocidos por todos los routers BGP, estos pueden ir en las actualizaciones pero no son incluidos en todas
- Atributos transitivos opcionales: Este tipo de atributos son reconocidos por algunos routers BGP y son anunciados sean o no reconocidos
- Atributos intransitivos opcionales: Este tipo de atributos son reconocidos por algunos routers BGP , si se recibe una actualización con este atributo, esta actualización debe ser anunciada sin lo atributos no reconocidos.

A continuación realizaremos una descripción de los Atributos BGP para su fácil comprensión y se ejemplificara el tipo de configuración a utilizar para realizar la ingeniera de trafico

4.3 Local Preference

El Local Preferecne es un atributo bien conocido visto como un valor local que posee un AS, este se utiliza para representar el grado de preferencia que posee un operador el cual es anunciado a través de sesiones BGP. Mientras mas alto sea el valor, mayor preferencia tendrá para su selección. De manera que este atributo se utiliza para indicar a un AS el camino o la ruta que tiene preferencia para salir del AS y así alcanzar una determinada red [1] . Para modificar este atributo de BGP se debe hacer uso de la herramienta de mapas de ruta para poder hacer la asociación de la modificación del local preference al peer con el cual se ha iniciado una sesión BGP.

La Figura 4 tiene 3 ASes en donde se trata de representar un escenario en el cual el AS 65100 recibe dos rutas para el prefijo 10.1.1.0/24, al ser mas corta la ruta por el enlace T1 este será elegido por default, de manera que se aplica un Local Preference de 200 al enlace OC3 de 200 y al enlace T1 se le aplica un Local Preference de 100 para influenciar el trafico a que elija el enlace OC3 para llegar al prefijo anteriormente mencionado.

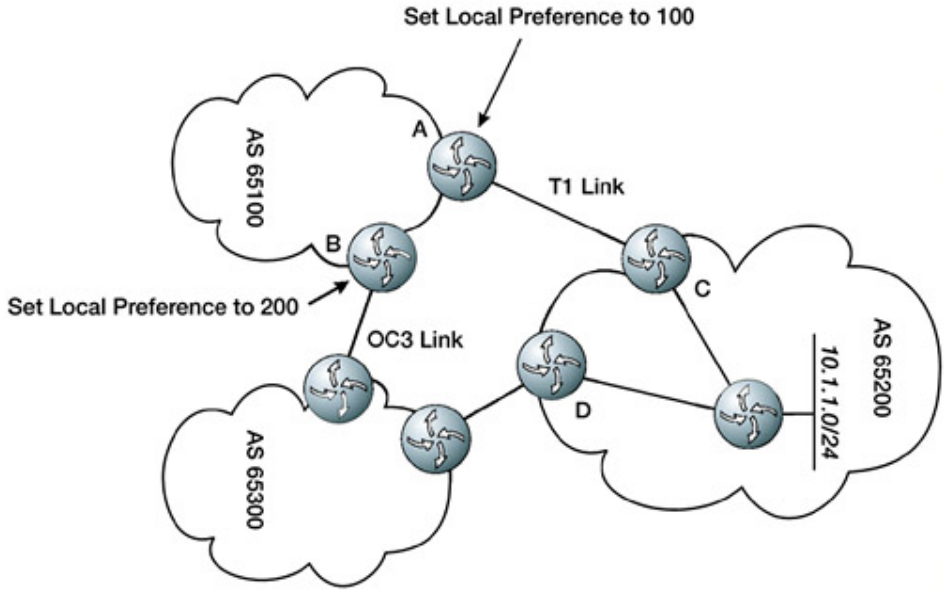

Figura 4: Local Preference [4]

En la Figura 5 se muestra la configuración de cómo editar el Local Preference aumentando el valor del AS 65300 para que este tenga preferencia sobre AS 65200, tenemos que utilizar los Mapas de Ruta para crear la política de encaminamiento asociadas a sus respectivas etiquetas "T1" y "OC3" y posteriormente asociar el Mapa de ruta a los vecinos para ejercer las políticas sobre sus respectivos enlaces. El valor por defecto del atributo de preferencia local es 100. Esta configuración se ha reducido a un solo router con dos enlaces solo para ejemplificar el modo de configuración.

```
!
router bgp 65100

 neighbor 192.0.254.17 remote-as 65200
 neighbor 192.0.254.17 route-map T1-in in
 neighbor 219.2.19.1 remote-as 65300
 neighbor 219.2.19.1 route-map OC3-in in
!
route-map T1-in permit 10
set local-preference 100
!
route-map OC3-in permit 10
 set local-preference 200
!
```

Figura 5: Configuración Local Preference[1]

4.4 Weight

Weight es un atributo BGP que se utiliza en el proceso de selección de ruta, el atributo se asigna localmente en el router, de manera que este valor solo tiene sentido para el router en especifico y no se propaga a través de las actualizaciones de rutas. El valor por defecto de Weight es "0" por lo tanto las rutas con un peso mas alto se prefieren. A diferencia del atributo Local Preference el cual es intercambiado entre routers del mismo AS, Weight solo es relevante localmente [1] .

En la figura 6 se muestra la configuración en donde se asigna un *weight* de valor 5000 al enlace del AS 40077 para que el prefijo 172.16.1.0/24 lo prefiera, y todo el trafico restante se deja con *weight* por default.

```
!
router bgp 65100
 neighbor 192.0.254.17 remote-as 65200
 neighbor 192.0.254.17 route-map T1-out out
 neighbor 219.2.19.1 remote-as 65300
neighbor 219.2.19.1 route-map OC3-out out
!
route-map T1-out permit 10
```

```
match ip address 2
set weight 5000
 !
 route-map T1-out permit 20
 !
 Access-list 2  permit 172.16.1.0 255.255.255.0
 i
```

Figura 6: Configuración Weight[1]

4.5 AS Path

AS Path es un Atributo bien conocido obligatorio con el cual se enlistan todos los ASes desde el origen hasta el destino, este tipo de Atributo es utilizado para dos cuestiones. Se utiliza para eliminar bucles en la red ya que si un equipo recibe una ruta con su mismo AS esta ruta es eliminada y también es utilizado para tomar decisiones en cuanto a políticas de encaminamiento, de manera que mientras menor sea al numero de AS-path listados para una ruta, mayor preferencia tendrá [1] .

Es por eso que con el Atributo *as-path* se puede realizar ingeniería de trafico de otra manera e influir en la selección de ruta anteponiendo su propio AS-path y realizando una extensión del atributo con múltiples copias de su propio número para agregar mas saltos, de este modo se influye en la elección ya que siempre se elegirá la ruta más corta.

A continuación se muestra en la Figura 7 la configuración con la obliga a preferir el enlace ispa para las rutas aprendidas por el AS 30088, anteponiendo su mismo AS 60055 varias veces en la lista de "4" sobre el AS 30088 para después hacer una coincidencia en el mapa de rutas y anteponer el AS 60055.

El comando *match* permite hacer la coincidencia del AS 30088 para así anteponer el AS 60055

```
i
ip as-path access-list 4 permit _30088_
ip as-path access-list 4 deny .*
!
route-map ispa-in permit 10
```

```
 set as-path prepend 60055
!
route-map ispb-in permit 10
 match as-path 4
 set as-path prepend 60055 60055 60055
!
route-map ispb-in permit 20
!
```

Figura 7: Configuración AS-path[1]

4.6 Next Hop

Este es Atributo bien conocido obligatorio contiene la dirección IP del siguiente salto en las actualizaciones cuando son enviadas fuera del AS. El atributo de siguiente salto también puede servir como una manera de dirigir el tráfico a otro equipo con el que se ha creado una sesión BGP, este debe ser configurado para declarar al vecino como siguiente salto en las sesiones BGP[4].

En la Figura 8 se muestra la configuración para declarar como Next Hop al vecino que es necesario para indicar el siguiente salto de la sesión BGP

```
!
route-map setnexthop permit 10
 set ip next-hop (Peer)
!
```

Figura 8: Configuración de Nex Hop [4]

4.7 Multi Exit Discriminator (MED)

Este es un atributo no transitivo opcional Anteriormente este Atributo era conocido como "Metric" y este fue diseñado para elegir una conexión cuando se tienen múltiples conexiones entre Sistemas Autónomos [4].

Este atributo de BGP nos da la capacidad de influenciar a un AS a preferir ciertas rutas asignando un valor menor de métrica en caso de tener varios enlaces para ese AS. MED solo puede ser utilizado entre dos Sistemas Autónomos vecinos de manera que no se anuncia mas allá del AS vecino, es por eso que se limita a lo mencionado anteriormente. Hay otros atributos importantes tales como *Weight, Local Preference, Originate Route, y AS path* que se toman en cuenta antes de considerar el atributo MED, por lo tanto, si cualquiera de estos criterios coincide, el atributo MED no será considerado [1] .

En la Figura 9 se muestra como el AS 62200 aplica un MED de 100 al enlace de salida T1 y un MED de 50 a su enlace de salida OC3, con esto se pretende que el AS 65100 elija el enlace OC3 para el prefijo 10.1.1.0/24.

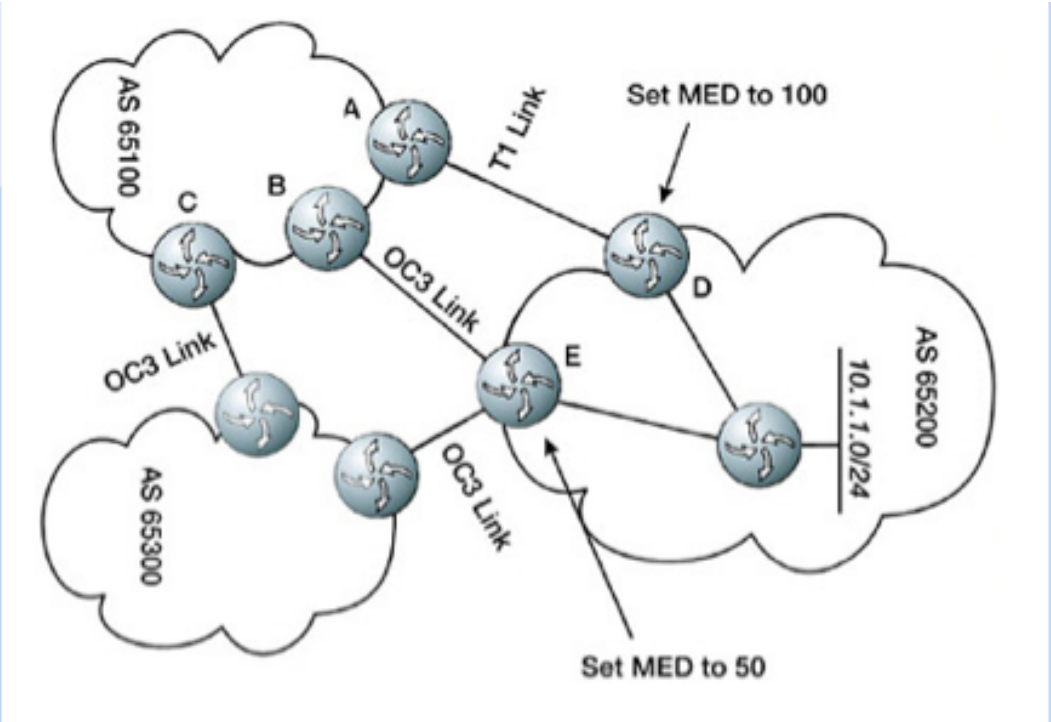

Figura 9: MED [4]

En la Figura 10 se utilizan los mapas de ruta para dar una etiqueta a cada enlace y asignar una métrica de manera que al asociarlos a un vecino con el cual se ha estableció sesión BGP se asignara la métrica para influenciar la selección de ruta.

```
!
router bgp 65100
 neighbor 192.0.254.17 remote-as 65200

 neighbor 192.0.254.17 route-map T1-out out

 neighbor 219.2.19.1 remote-as 65200
 neighbor 219.2.19.1 route-map OC3-out out
!
route-map T1-out permit 10
 set metric 100
!
route-map OC3-out permit 10
 set metric 50
!
```

Figura 10: Configuración MED[1]

4.8 Origin

El origen es un atributo obligatorio bien conocido que indica el origen del prefijo o, más bien, la forma en que el prefijo se inyectó en BGP. Hay tres códigos de origen, en orden de preferencia [1] :

- IGP, es decir, el prefijo se originó a partir de información obtenida de un protocolo de gateway interior.

- EGP, es decir, el prefijo se originó a partir del protocolo EGP, que sustituye BGP.

- INCOMPLETO, es decir, el prefijo se originó de una fuente desconocida.

Este Atributo solo es para identificar la fuete o el origen del anuncio BGP, ya que puede provenir de un IGP, EGP u otros como normalmente resultan de la agregación, la redistribución, u otras formas indirectas de la instalación de rutas en BGP el cual seria marcado como Incompleto, con este Atributo no se realiza nada en la practica pero es obligatorio.

4.9 Comunidades

Este Atributo no es utilizado en el proceso de selección de ruta pero se puede utilizar para definir acciones. Una comunidad es una asociación de un AS con un valor, el cual puede ser expresado como 100:101, de manera que 100 seria el numero de AS y 101 es un valor que se añade el cual tiene un significado dentro del AS. Es decir, una comunidad es un grupo de prefijos que comparten alguna característica común, y puede ser configurado con el atributo de comunidad BGP, estas se pueden utilizar para realizar Ingeniería de Tráfico, en si las Comunidades no alteran el proceso de toma de decisiones de BGP, sino se utilizan como identificadores con el fin de marcar rutas. Esto se realiza mediante la asociación sistemas autónomos y un valor asignado, de esta manera que se puedan identificar las rutas procedentes de dicha asociación, posteriormente se puede asignar un valor de Métrica y Local Preference para dar o no dar preferencia a los mismos [1] .

En la Figura 11 se muestra la configuración mediante el comando *ip community-list* hay dos comunidades que asocian dos valores diferentes con el AS 50066, también se utiliza el mapa de ruta para asignar los valores de Métrica y Preferencia Local, en el supuesto de que la ruta haya sido recibida por dos enlaces, lo que estamos buscando es que las rutas de la comunidad 50066:3001 prefieran enlace ispb asignando un mayor Local Preference y baja Metrica y rutas que proviene de la comunidad 50066:3002 se les da una métrica más alta para así descartar el utilizar el enlace ispba. Se deja todo el trafico restante con la misma métrica para que BGP realice su selección de ruta normal.

```
!
router bgp 60055
 bgp always-compare-med
!

ip bgp-community new-format
ip community-list 1 permit 50066:3001
ip community-list 1 deny
ip community-list 2 permit 50066:3002

ip community-list 2 deny
!
route-map ispa-in permit 10
 set metric 10
!
route-map ispb-in permit 10
 match community 1
 set metric 10
 set local-preference 120
!
route-map ispb-in permit 20
 match community 2
 set metric 20
!
route-map ispb-in permit 30
 set metric 10
!
```

Figura 11: Configuración de Comunidades[1]

2.4 Filtrado de Rutas

Con BGP puede realizar el filtrado de rutas ya que en muchos casos es necesario evitar un aumento enorme en la tabla de encaminamiento y sólo utilizar las rutas necesarias, el filtrado de rutas también se puede utilizar solamente para descartar rutas que no necesitemos. Un ejemplo muy claro se puede presentar en la conexión que tienen entre ISPs de clasificación Tier 1, ya que la conexión es solo para intercambiar transito que necesitan, de manera que no les interesa recibir toda la información de encaminamiento del vecino sino solo unas rutas por las cuales se hace el intercambio o la conexión. El filtrado puede realizarse de diferentes maneras.

2.4.1 Filter List

Estas listas basadas en el atributo AS-Path se utilizan para restringir o aceptar rutas, para configurarlas hay que añadir los Sistemas Autónomos a través del cual viaja la ruta y se puede delimitar aun mas utilizando expresiones regulares, también se debe asociar un *filter-list* al vecino con el cual se ha levantado una sesión BGP [1] .

En la Figura 12 se muestra la configuración a utilizar para crear una Filter list.

```
!
router bgp 60055
 neighbor 192.0.254.17 filter-list 1 in
!
ip as-path access-list 1 deny .+_.+_.+_.+_.+_.+_.+
ip as-path access-list 1 permit .*
!
```

Figura 12: Configuración Filter List[1]

2.4.2 Distribution Lists

Estas listas filtran rutas basadas en las direcciones IP de destino u origen, funcionan como listas de acceso en la que se pueden declarar las direcciones IP o rangos de direcciones. En general, son más eficaces que Filter List, ya que se basan en los prefijos y no en el AS-Path [1] . A continuación en la Figura 13 se muestra la configuración a realizar para los dos tipos de configuraciones en caso de usar listas de acceso estándar o extendidas, nótese que para la configuración de las listas es necesario utilizar una wildcard en lugar de la mascara de red.

```
!
router bgp 60055
 neighbor 192.0.254.17 distribute-list 10 in
!
access-list 10 deny   10.0.0.0 0.255.255.255
access-list 10 deny   172.16.0.0 0.15.255.255
access-list 10 deny   192.168.0.0 0.0.255.255
access-list 10 permit any
!
router bgp 60055
 neighbor 192.0.254.17 distribute-list 110 in
!
access-list 110 deny   ip 128.0.0.0 0.255.255.255 255.255.128.0 0.0.127.255
access-list 110 permit ip any any
!
```

Figura 13: Configuración Distribution List[1]

2.4.3 Prefix List

El prefix-list funcióna como una lista de acceso la cual contiene una o mas entradas las cuales son procesadas de manera secuencial, esta secuencia se declara en la configuración[1] . En la configuración que se muestra en la Figura 14 se crean un prefix-list con la etiqueta *infilter,* se declaran varias entradas de manera secuencial las cuales contienen los prefijos o rango de prefijos que se quieren anunciar al vecino con el cual se levanto una sesión BGP.

```
!
router bgp 60055
 neighbor 192.0.254.17 prefix-list infilter in
!
ip prefix-list infilter description inbound filter
ip prefix-list infilter seq 5 permit 0.0.0.0/1 le 20
ip prefix-list infilter seq 10 permit 128.0.0.0/2 le 20
```

```
ip prefix-list infilter seq 15 permit 192.0.0.0/3 le 24
!
```

Figura 14: Configuración Prefix List[1]

Todas las técnicas anteriormente vistas son bastante dinámicas ya que al asociar cualquier técnica al vecino se pueden filtrar las rutas de entrada o de salida cambiando el comando de "in" por "out".

2.5. BGP en grandes redes

2.5.1 Escalabilidad con BGP

BGP es un protocolo eficiente, extensible y escalable, pero cuenta con una limitación muy importante y esta es que todos los routers dentro de un AS deben tener una sesión iBGP con cualquier otro router BGP en el AS, esto es debido a la regla para prevención de bucles dentro de una red iBGP ya que iBGP no cuenta con el atributo AS-path como es el caso de eBGP por lo tanto las rutas iBGP aprendidas no son propagadas con los vecinos iBGP, es por eso que en caso de que un router de borde reciba una actualización proveniente de una sesión eBGP tiene que enviar esta actualización hacia la red interna en donde se esta utilizando iBGP de manera que para enviar esta actualización lo debe hacer mediante todas las sesiones BGP que haya creado con los equipos de la red interna y para que todos los equipos puedan recibir estar actualización es necesario que haya una red completamente mallada. Para esta cuestión se han propuesto dos tipos de arquitectura o configuraciones las cuales permiten resolver este problema de escalabilidad, estas son "*Reflectores de Rutas y Confederaciones*" [1] .

2.5.2 Reflector de rutas

Un Reflector de rutas permite romper la regla de tener una red completamente mallada, ya que estos pueden enviar todas las actualizaciones de una sesión iBGP a otros equipos dentro de la red iBGP los cuales pueden ser llamados "Clientes o no Clientes", de manera que los routers BGP solo deben tener una sesión iBGP con el Reflector de rutas y ellos reciben la mejor ruta la cual ha sido determinada por el

Reflector de rutas, Los enlaces que puede tener un Reflector de rutas tienen dos clasificaciones "clientes y no clientes". El Reflector de rutas y sus clientes forman un "Cluster" y todos los demás enlaces que tiene el Reflector de rutas que no son parte del Cluster funcionan como cualquier iBGP clásico de manera que no trabajan con las funcionalidades que ofrece el Reflector de rutas [1] .

Los Reflectores de rutas trabajan con dos atributos muy importantes para anunciar las actualizaciones, *"Originator id" y "Cluster id"* , estos dos parámetros van dentro de las actualizaciones para así poder prevenir bucles, ya que así logra identificar si recibe mas de una actualización para el mismo destino y puede realizar la elección de la mejor ruta.

El Cluster id es un atributo que contiene una lista de identificadores de cada router por el cual ha viajado una ruta reflejada, el cluster id por defecto es el ID del reflector de rutas o también puede ser algún valor previamente configurado. Cuando un reflector de ruta recibe una ruta de alguno de sus clientes fija el *originator id* con el valor del *router id* del cliente que origino la ruta [1] .

Cuando un reflector de rutas refleja las rutas recibidas, nuca deberá cambiar los atributos de Next hop, Local Preference, MED o el AS Path que están asociados con la ruta, ya que al cambiar estos podría generarse un bucle en la red [1] .

Al implementar Reflectores de ruta en una red se crea un punto único de falla por lo tanto si llegara a fallar el reflector de rutas se perderá la comunicación entre las sesiones iBGP, para evitar que se genere este escenario es necesario tener reflectores de ruta redundantes con los clientes y tener un buen diseño de red. Un cliente debe tener sesiones iBGP con mas de un Reflector de rutas para evitar el punto único de falla. Al tener sesión con uno o mas Reflectores de ruta el cliente recibe rutas de los dos reflectores y los reflectores reciben las rutas del mismo cliente que da como resultado dos copias de la misma ruta en los dos casos.

El comando a utilizar para realizar clúster de reflectores de ruta es *"bgp cluster-id ID"* el cual solo se deberá configurar en cada reflector de rutas con un valor igual o diferente dependiendo de si queremos que las rutas sean duplicadas o no y así poder identificarlas

El Reflector de rutas sigue las siguientes reglas

- Si la ruta se ha recibido de un "no cliente" la ruta es reflejada a todos sus clientes [4].

- Si la ruta se ha recibido de un "cliente" , la ruta es reflejada a todos sus clientes y no clientes [4].

La Figura 15 muestra una ejemplo de una red diseñada con un reflector de ruta el cual tiene como cliente a cuatro equipos (B, E, C y F), los cuales tienen comunicación entre ellos sin necesidad de estar directamente conectados el uno con el otro.

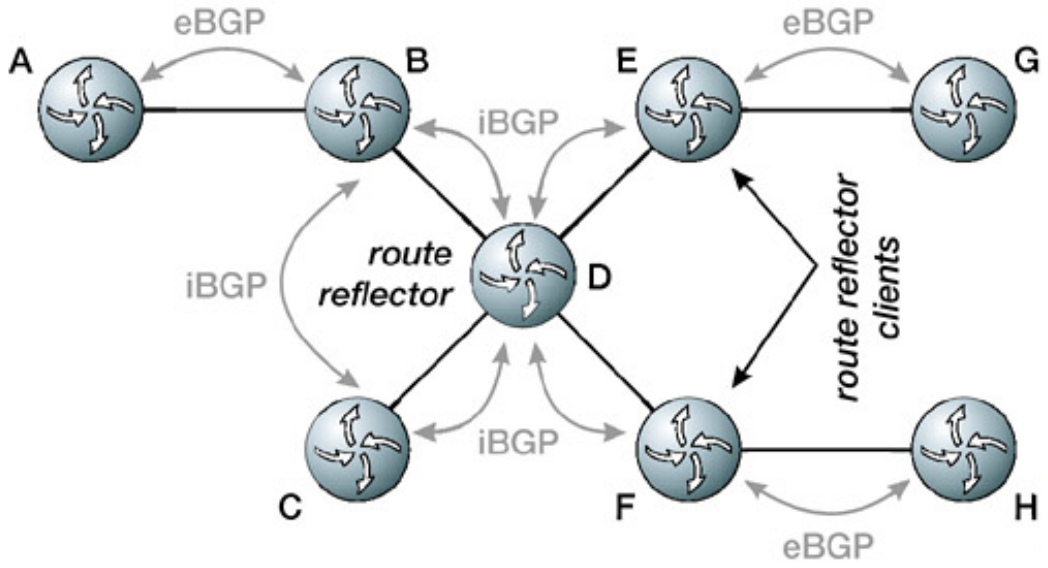

Figura 15: Diseño red reflectores de ruta [4]

En la Figura 16 se muestra la configuración necesaria para establecer un equipo como Reflector de ruta y sus vecinos por medio de un *Group peer* para simplificar la configuración

```
!
router bgp 60055
 bgp cluster-id 257
 neighbor rrclients peer-group
 neighbor rrclients remote-as 60055

 neighbor rrclients route-reflector-client
 neighbor 192.0.2.66 peer-group rrclients
 neighbor 192.0.2.66 description BR2
 neighbor 192.0.2.67 peer-group rrclients
 neighbor 192.0.2.67 description BR1
!
```

Figura 16: Configuración Reflector de rutas[1]

2.5.3 Confederaciones

Las confederaciones es otra solución propuesta para evitar la malla completa, para este caso se propone dividir la red en subsistemas autónomos (sub-Ases) pero todos dentro de una confederación, de manera que para el exterior los sub-Ases dentro de la confederación se verán como un único AS utilizando un identificador para marcar toda la red hacia el exterior y dentro de cada sub-AS se utilizaran números de AS diferentes que solo serán validos a nivel local. Al implementar una confederación se tendrá que hacer uso de reglas iBGP y eBGP , ya que dentro de los sub-ASes se debe un iBGP completamente mallado y para la comunicación entre sub-ASes se levantaran sesiones eBGP las cuales son muy parecidas a las clásicas sesiones eBGP. Debido a que en eBGP se trabaja con el atributo AS-path, entre las sub-ASes también se utiliza el AS-path anteponiendo cada sub-AS su propio numero de AS, de esta manera se evita genera bucles dentro de la red, pero cuando un router quiere enviar información fuera de la confederación a una sesión eBGP la cual fue levantada con un vecino con AS diferente en el exterior de la red, no se envía ningún AS-path de los sub-ASes, sino se envía un único identificador el cual es el numero de AS de la red total asignado [1] .

En las confederaciones se tienen dos nuevos atributos los cuales son utilizados para la prevención de bulces y van dentro del AS path:

- AS Confederation Sequence: Este atributo es una lista con el orden de todos los sistemas autónomos por los cuales ha pasado una ruta dentro de una confederación [4].
- AS Confederation Set: Es una lista de todos los sistemas autónomos por los cuales ha pasado una actualización, solo que es lista no tiene un orden en particular[4].

Las reglas que siguen las confederaciones al modificar una actualización son:

- Si se anuncia una actualización a un enlace iBGP normal sigue el proceso normal[4].
- Si se advierte a un enlace eBGP el cual esta dentro de una confederación y comparten el ID de confederación, antepone su numero de AS en la lista de ASes, del atributo AS Confederation Sequence [4].
- Si se anuncia a un enlace eBGP el cual esta fuera de la confederación y no comparte el ID de confederación, quita el AS Confederation Sequence y el AS Confederation Set y antepone el ID de Confederación único a la secuencia de AS que contiene el AS Path [4].

En la Figura 17 se muestra un red la cual ha sido diseñada con confederaciones, en ella podemos ver que el AS 65500 cuenta con dos subsistemas (65200 y 65300) de manera con esta configuración se reducen la cantidad de enlaces iBGP y se con comunicación y anuncio de rutas para los equipos dentro de este AS.

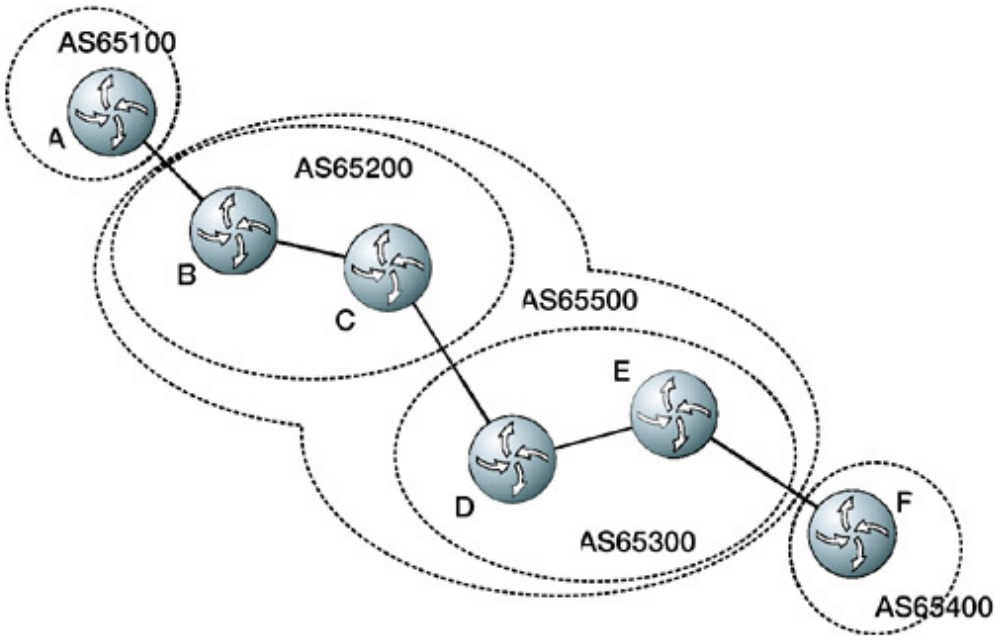

Figura 17: Diseño de red con confederaciones [4]

2.5.4 Actualizaciones con Interfaces Virtuales Loopback

El uso de una interfaz de loopback para establecer vecinos es común con iBGP, pero no es común con eBGP. Cuando se crea una sesión con un vecino BGP, BGP utiliza la dirección IP de la interfaz por defecto para establecer la conexión TCP, en el caso de eBGP eso es bueno porque si se caen interfaces deben ser haber una notificación de que ya no existen esos enlaces y se debe reflejar en la topología [1] .

Para iBGP es necesario asociar la sesión de BGP en una interfaz de loopback, de manera que si una interfaz se desactiva, la sesión BGP permanece activa y el IGP puede calcular la ruta alterna, el comando que se utiliza para hacer la asociación sería update-source loopback0. En la Figura 18 se muestra la configuración necesaria para habilitar esta función.

```
!
interface Ethernet0
 ip address 192.0.2.67 255.255.255.192

 no ip directed-broadcast
!
interface Loopback0
 ip address 192.0.2.144 255.255.255.255
 no ip directed-broadcast
!
router bgp 60055
 no synchronization
 neighbor 192.0.2.145 remote-as 60055
 neighbor 192.0.2.145 update-source Loopback0
!
```

Figura 18: Configuración Update Loopback[1]

2.5.5 Peer Groups

Los router BGP pueden tener muchos vecinos los cuales pueden tener configuración en común, una característica que tiene BGP es que la configuración en común de varios vecinos BGP se puede agrupar y ser asociada a todos los vecinos para así acortar la configuración y tener un orden, en lugar de configurar los vecinos uno por uno [1] .

2.5.6 BGP Compatible con IGP

BGP es un protocolo que puede convivir con otros Protocolos de Gateway Interior, incluso de puede redistribuir información de estos protocolos por medio de BGP par influir en la toma de decisiones respecto a las rutas a seleccionar o ser distribuido. En la Tabla 6.1 se muestra la distancia administrativa de cada protocolo únicamente para mostrar el peso que tiene cada protocolo en el encaminamiento, mientras menor sea el valor, mayor preferencia tendrá.

Routing Protocol	Administrative Distance
Directly Connected	0
Static	1
External BGP	20
Internal EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
External EIGRP	170
Internal BGP	200

Tabla 1. Distancia Administrativa de los protocolos de encaminamiento

3. Implementación de una red BGP

Al ya haber realizado un estudio de las características y capacidades del protocolo BGP, se pretende implementar una red BGP con la cual se ejemplificara algunas de las características mas importantes y su funcionamiento.

Para la implementación de la red se hizo uso de diferentes herramientas como es el caso de VNX y Quagga, ya que para emular una red que consta de equipos y protocolos IP es necesario la virtualización de maquinas y emulación de los equipos de datos. A continuación se dará una breve introducción a estas herramientas para su mejor compresión pero no se indagara mucho en el tema que ya la documentación es muy amplia.

3.1 Virtual Networks over LinuX (VNX)

VNX es una herramienta desarrollada por el Grupo de Investigación de Telecomunicaciones, Redes de Internet y Servicios el cual pertenece al Departamento de Ingeniería Telemática de la Universidad Politécnica de Madrid. Esta es una herramienta de código libre o abierto la cual es utilizada para virtualización permitiendo crear redes virtuales para la realización de escenarios de pruebas. VNX crea los escenarios de red a partir de maquinas virtuales de diferentes tipos ya sean Linux, Windows, FreeBSD, Olive o Dynamips los cuales dependiendo del diseño de red que proponga el usuario tendrán una función especifica [3].

VNX es muy útil para probar aplicaciones, servicios de red a través de nodos y redes virtuales ya que con ella se pueden crear laboratorios de redes muy simples hasta redes complejas similares a las actuales emulando comportamientos reales que se pueden presentar en la operación de las mismas. Esta herramienta es similar a otras existentes como GNS3, Nekit, MLN, etc [3].

VNX consta de un lenguaje XML el cual permite describir el escenario de red virtual, también cuenta con una versión distribuida que permite el despliegue de escenarios virtuales a través de grupos de servidores Linux. La documentación completa de VNX se encuentra en: http://web.dit.upm.es/vnx:iki/index.php/Main_Page

3.2 QUAGGA

Quagga es una suite que contiene software de enrutamiento para proporcionar implementaciones y funciones de los diferentes protocolos como OPSFv2, OSPFv3, RIP v1 y v2, RIPng y BGP-4 a las plataformas Unix, especialmente FreeBSD, Linux, Solaris y NetBSD. En la Tabla 7.1 se muestra los diferentes protocolos que soporta Quagga [2].

IPv4	IPv6	
Zebra		interfaz del kernel, rutas estáticas, servidor zserv
Ripd	Ripngd	RIPv1/RIPv2 para IPv4 y RIPng para IPv6
Ospfd	Ospf6d	OSPFv2 y OSPFv3
Bgpd		BGPv4 + (incluyendo soporte para multicast e IPv6)
Isisd		IS-IS con soporte para IPv4 y IPv6
Babeld		BABEL enrutamiento inalámbrico (IPv4 e IPv6)
Olsrd		OLSR enrutamiento inalámbrico a través de un plug-in para olsrd
Ldpd		MPLS Label Distribution Protocol
bfdd		Bidirectional Forwarding Detection

Tabla 2: Protocolos soportados por Quagga [2]

Los demonios de Quagga pueden ser configurados a través de una CLI llamado vty, el cual es similar a la línea de comandos de un router común. También tiene una herramienta llamada "vtysh" la cual es un acceso general a todos los demonios de Quagga y permite administrar casi a todos.

La documentación completa de Quagga se encuentra en: http://www.nongnu.org/quagga/.

3.3 Diseño General de la Red

En la Figura 19 se muestra la red BGP que se pretende implementar la cual ha diseñado jerárquicamente para poder dar un simple ejemplo de cómo están conectadas las redes actualmente en el mundo, en este caso se han divido los IPSs en sistemas autónomos para poder delimitar bien el alcance de cada uno y detallar las funciones que desempeñan dentro de la red y su diseño

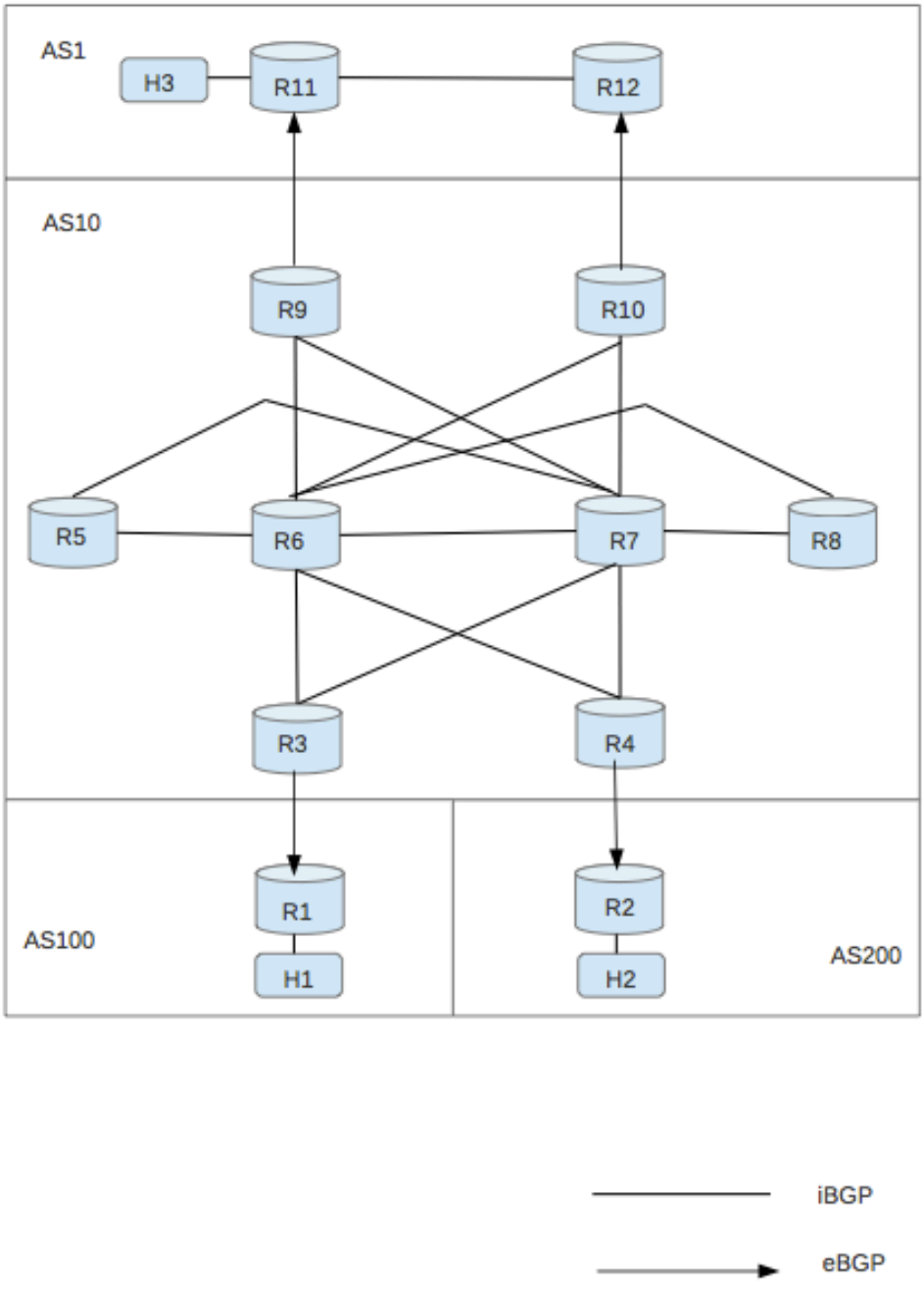

Figura 19: Red BGP completa

En la Figura 19 se presenta la red completa BGP la cual cuenta con 4 sistemas autónomos, estos a su vez representan Tier 1, 2 y 3 en orden descendente, se ha utilizado el prefijo 10.0.0.0/16 para la configuración de las interfaces de cada equipo dentro de la red BGP.

La red cuenta con los dos tipos de instancias BGP las cuales son eBGP e iBGP. Los dos diferentes tipos de protocolo BGP se utilizan dentro de la red para la conexión e intercambio de información dentro de los ASes y entre ellos; dependiendo del diseño de cada AS se utilizaran las variantes de BGP para tener conectividad entre los equipos y realizar un diseño eficiente.

Para poder explicar mejor el diseño de la red se presentaran diferentes tablas con los parámetros de cada sistema autónomo y se explicara el diseño de red que utiliza cada uno, de manera que se hará un desglose de la red completa en orden jerárquico por Tier para poder describir con detalle como opera cada sistema autónomo y su diseño.

3.4 Desglose de Red

3.4.1 Tier 3

En esta parte de la red, en la Figura 8.1 y en la Tabla 8.1 se muestra el segmento de red el cual comprende los Sistemas Autónomos 100 y 200 con los equipos que pertenecen a la jerarquía Tier 3. Nos podemos percatar que el protocolo que se esta utilizando es la variante eBGP ya que como se muestra en la Imagen 6 solo cuentan con comunicación al exterior de su propio sistema autónomo por lo que el protocolo a utilizar es BGP externo, el cual hace uso del atributo AS-Path en las actualizaciones que se envían a los vecinos para anteponer el numero de AS y empezar a trazar la ruta en la red para el prefijo que están anunciando, de esta manera se evita generar un bucle en la red y se identifica la procedencia del prefijo anunciado hacia la red exterior.

En este caso se presentan estos equipos como Tier 3 para ejemplificar proveedores chicos los cuales se conectan con otros proveedores de mayor magnitud en su red para tener conectividad con otros AS, la conectividad se realiza por medio de enlaces punto a punto en los cuales ha sido configurada la instancia eBGP en cada uno asociando el AS de la red con la que se intenta comunicar; en este caso seria el AS 10. A su vez se ha configurado en cada equipo una interface LAN para realizar pruebas de host a host.

Para la LAN de R1 se ha asignado el direccionamiento 10.1.1.0/24 y para la LAN de R2 se asigno el direccionamiento 10.2.1.0/24. En la Figura 20 se presenta el diseño de red para este segmento

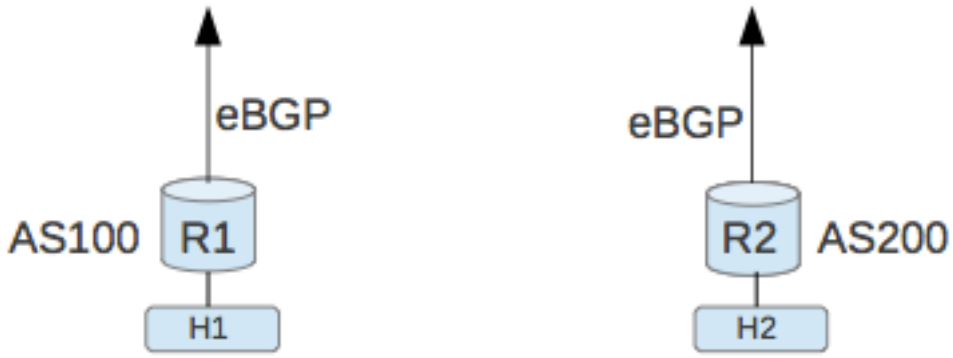

Figura 20: Tier 3 Sistemas Autónomos 100 y 200

En la Tabla 3 se muestran los componentes de cada equipo como las interfaces, la instancia de BGP que se utiliza en cada una de ellas y el AS al que pertenecen

Equipo	Tipo de equipo	Interfaces	Direccionamiento	Tipo de BGP	AS	Diseño de red
R1	BGP	eth1	10.1.1.1/24	Lan A	100	PtP
		eth2	10.3.1.1/30	eBGP		
		lo0	10.1.0.1/24			
R2	BGP	eth1	10.2.1.1/24	Lan B	200	PtP
		eth2	10.3.1.5/30	eBGP		
		lo0	10.2.0.1/24			

Tabla 3: Parámetros Tier 3

3.4.2 Tier 2

Reflectores de ruta

En esta parte de la red se implemento un diseño BGP de Reflector de Ruta con Clusters para obtener redundancia en la red interna del Tier 2 el cual cuanta con el numero de Sistema Autónomo 10, como se menciono anteriormente ese diseño se ha escogido ya que de esta manera se reducen los enlaces iBGP los cuales en un escenario sin reflectores de ruta están obligados a realizar una red completamente mallada entre todos los equipos con enlaces iBGP, por lo que con este diseño se vuelve mas escalable la red; de igual manera la red presenta enlaces eBGP para conectar con las redes fuera del AS ya sea para conectarse con un proveedor mas grande que ofrece interconexión o con algún cliente al que se le brinda servicio de interconexión. Con esta red se pretende representar un proveedor de clasificación Tier 2 el cual consta de una magnitud mayor que las redes a las que presta servicio de conexión.

En la Figura 21 se muestra un diseño de red con 8 routers interconectados por medio de iBGP y con conexiones eBGP para conectarse al exterior del AS, al la red se le ha asignado el numero de AS 10. Para la parte del diseño de los reflectores de ruta se consideraron los equipos R6 y R7 los cuales funcionan como reflectores de todos los demás equipos de la red contando con un enlace a cada equipo, cada uno forma parte de un Cluster al cual se le asocian clientes que son los routers a los que se le anunciaran las rutas; con el diseño de Cluster se logra tener redundancia ya que se tienen dos equipos trabajando como reflectores de rutas y en caso de que llegara a fallar un reflector, se mantiene la conectividad con el equipo secundario, de manera que los equipos R3, R4, R5, R8, R9 y R10 serán cliente de R6 y R7 y cuentan con enlaces a cada uno de los reflectores para así lograr la redundancia requerida. Como se menciono anteriormente en el estudio de BGP en este tipo de diseño de red implementado reflectores de ruta los atributos a utilizar para crear una red libre de bucles serán *"Originator id" y "Cluster id"* , de manera que los equipos R6 y R7 que trabajan como reflectores son los encargados de gestionar el envió de rutas aprendidas de sus clientes o equipos directamente conectados a todos los demás equipos dentro de la red y con los atributos mencionados se logra crear una red sin bucles ya que de esta manera se identifica la procedencia de la ruta y se realiza su elección.

Para el equipo R6 el cual trabaja como reflector se le ha asignado el Cluster ID 1.1.1.1 y para R7 el cual también trabaja como reflector se le ha asignado el Cluster ID 2.2.2.2; el comando utilizado es *"bgp cluster-id (ID)"*. El comando utilizado para la asociación de clientes a los equipos que trabajan como reflectores es *"neighbor (peer) route-reflector-*

client". Cabe mencionar que esta configuración debe ser agregada en la parte de BGP del equipo que trabaja como reflector solamente, en los clientes no habrá que agregar configuración adicional

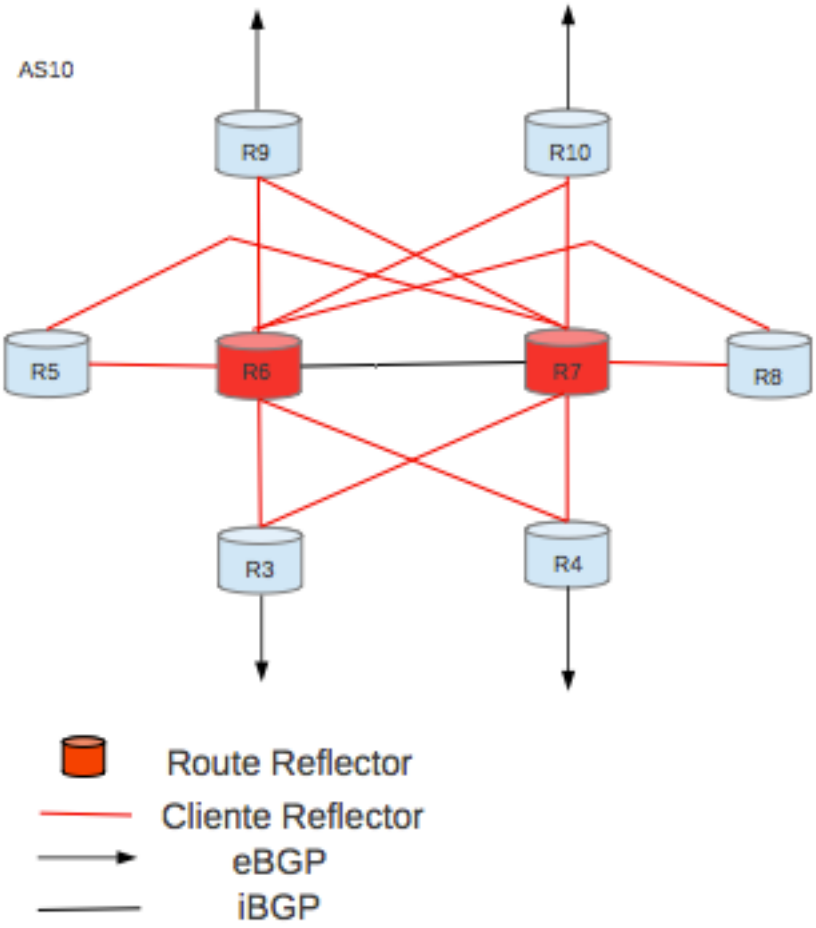

Figura 21: Tier 2 Sistema Autónomo 10

En la Tabla 4 muestran los parámetros de configuración que contiene el diseño de red con routers reflector en el cual se detalla que función desempeñan los equipos dentro de la red, las interfaces que se han dado de alta en los equipos, el direccionamiento asignado a cada una de sus interfaces, la variante de BGP con la que están trabajando las interfaces para conectar con sus vecinos, el AS al que pertenecen y en que diseño de red están trabajando.

Equipo	Tipo de equipo	Interfaces	Direccionamiento	Tipo de BGP	AS	Diseño de red
R3	Cliente BGP/BGP	eth1	10.3.1.2/30	eth1	10	Route Reflector
		eth2	10.3.1.9/30	eth2		
		eth3	10.3.1.13/30	eth3		
		lo0	10.3.0.1/24			
R4	BGP	eth1	10.3.1.6/30	eBGP	10	Full Mesh
		eth2	10.3.1.17/30	iBGP		
		eth3	10.3.1.21/30	iBGP		
		lo0	10.3.0.2/24			
R5	Cliente BGP	eth1	10.3.1.26/30	iBGP	10	Route Reflector
		eth2	10.3.1.53/30	iBGP		
		lo0	10.3.0.3/24			
R6	Router Reflector/BGP	eth1	10.3.1.10/30	iBGP	10	Router Reflector/Full Mesh
		eth2	10.3.1.25/30	iBGP		
		eth3	10.3.1.29/30	iBGP		
		eth4	10.3.1.33/30	iBGP		
		eth5	10.3.1.37/30	iBGP		
		eth6	10.3.1.18/30	iBGP		
		eth7	10.3.1.57/30	iBGP		
		lo0	10.3.0.4/24			
R7	Router Reflector/BGP	eth1	10.3.1.22/30	iBGP	10	Router Reflector/Full Mesh

		eth2	10.3.1.14/30	iBGP		
		eth3	10.3.1.38/30	iBGP		
		eth4	10.3.1.41/30	iBGP		
		eth5	10.3.1.45/30	iBGP		
		eth6	10.3.1.49/30	iBGP		
		eth7	10.3.1.54/30	iBGP		
		lo0	10.3.0.5/24			
R8	Cliente BGP	eth1	10.3.1.50/30	iBGP	10	Route Reflector
		eth2	10.3.1.58/30	iBGP		
		lo0	10.3.0.6/24			
R9	BGP	eth1	10.3.1.30/30	iBGP	10	Full Mesh
		eth2	10.4.1.6/30	eBGP		
		eth3	10.3.1.42/30	iBGP		
		lo0	10.3.0.7/24			
R10	Cliente BGP/BGP	eth1	10.3.1.46/30	iBGP	10	Route Reflector
		eth2	10.3.1.34/30	eBGP		
		eth3	10.4.1.10/30	eBGP		
		lo0	10.3.0.8/24			

Tabla 4: Parámetros Tier 2

3.4.3 Tier 1

Por ultimo en esta parte de la red se presenta el segmento clasificado como Tier 1 el cual tiene asignado el Sistema Autónomo numero 1 y solo consta de dos routers R11 y R12 , estos se comunican hacia el exterior por medio de eBGP y entre ellos se

comunican por un enlace iBGP. Esta parte de la red representan un proveedor el cual brindaría interconexión mas allá de la red del proveedor de Tier 2 el cual necesita de los servicios de un proveedor de clasificación Tier 1 para conectarse a nivel internacional ya que su infraestructura o red tienen alcance a nivel nacional o local. Se ha asignado una interface LAN a R11 con el segmento 10.5.1.0/24 para realizar pruebas de host a host y poder verificar el comportamiento de trafico que presenta la red. En la Figura 22 se muestra el diseño de red y como se interconectan los equipos R11 y R12.

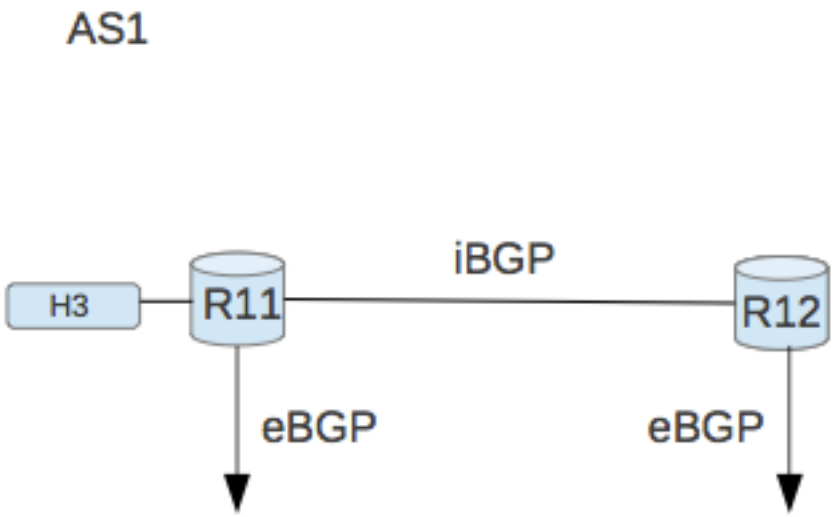

Figura 22: Tier 1 Sistema Autónomo 1

En la Tabla 5 se muestran los parámetros que comprenden esta parte de la red, identificando los equipos dentro de la red, las interfaces que posee cada equipo, el direccionamiento asignado a las interfaces, el numero de AS al que pertenecen y la instancia BGP con la cual están trabajando

Equipo	Tipo de equipo	Interfaces	Direccionamiento	Tipo de BGP	AS	Diseño de red
R11	BGP	eth1	10.4.1.5/30	eBGP	100	PtP
		eth2	10.4.1.1/30	iBGP		

		lo0				
R12	BGP	eth1	10.4.1.9/30	eBGP	200	PtP
		eth2	10.4.1.2/30	iBGP		
		eth3	10.5.1.1/24			
		eth1	10.4.1.9/30			

Tabla 5: Parámetros Tier 1

Con la implementación de esta red se pretende tener conectividad dentro de toda la red entre todos los equipos solo utilizando el protocolo BGP. Por medio de los reflectores se da solución a la forzosa implementación de una red completamente mallada cuando se hace uso de la instancia iBGP, al implementar Clusters se obtiene redundancia en la red y se ejemplifica de una manera muy general como es la interconexión en la actualidad de los diferentes proveedores que prestan servicio de telecomunicaciones en el mundo.

3.5. Ingeniería de Trafico

Para la manipulación del trafico en el borde de la red de Tier 2 el cual tiene como conexión a la red Tier 1 se han utilizado los atributos que ofrece BGP y en este caso en especifico se utilizo el Local Preference para marcar las rutas que entran a la red y MED para marcar las rutas que salen de la red.

Utilizando estos atributos se intenta ejemplificar como seria la elección de enlaces o la manipulación de trafico para adecuar el trafico de red dependiendo de las necesidades de la red o del servicio que se necesita ofrecer. Para realizar la asociación de la modificación de los atributos se ha utilizado los Mapas de Ruta, asi de esta manera en la configuración de peers en BGP se puede asociar el mapa de ruta con la modificación del atributo al peer del cual estamos recibiendo rutas o estamos enviando rutas.

3.5.1 Local Preference

Como se menciono en el estudio de BGP realizado mientras mayor sea el valor de Local Preference mayor prioridad tendrá el anuncio; por defecto el valor de Local Preference tiene un valor de 100 de manera que en la red Tier 2 a los anuncios entrantes por parte del equipo R12 se le ha asignado un Local Preference de 500 para que el enlace de R10 hacia R12 para el trafico saliente tenga mayor prioridad que el enlace de R9 hacia R11.

El atributo ha sido modificado utilizando el comando *"set local-preference (valor)"* agregando un valor el cual queremos que adquiera el atributo para después ser asociado a un route map y posteriormente asociar el route map al peer del cual se reciben rutas

3.5.2 MED

Para el marcado de las rutas anunciadas hacia fuera de la red Tier2 enviadas a la red Tier1 las cuales cuentan con dos enlaces para el intercambio de trafico se ha utilizado el atributo MED para marcar los prefijos enviados hacia R11 y R12. Para realizar el marcado de los prefijos enviados por los dos enlaces hacia el Tier 1 se modifica la métrica de lo mismo asignando valores de 200 a los prefijos enviados por el enlace entre R9 y R11 y se le asigna un valor de 50 a los prefijos enviados por el enlace entre R10 y R12.

Con este atributo la preferencia se da con el menor valor asignado de manera que las rutas marcadas con el valor de 50 tendrán preferencia sobre las que estén marcadas con 200. El comando utilizado para la modificación del atributo es *" set metric (valor)"* asignando un valor para después ser asociado a un mapa de ruta y este posteriormente ser asociado al peer en la configuración de BGP con el cual se intercambia trafico.

4. Resultados generales de la red

4.1 Resultados

Al implementar la red propuesta se obtuvieron los siguientes resultados:

1. La red es configurable al 100%
2. Presenta escalabilidad
3. La red presenta conectividad completa entre todos los equipos y hosts
4. Con el diseño de reflectores de ruta se reduce el numero de enlaces iBGP
5. La red presenta redundancia en cuanto a reflectores de ruta como equipos BGP
6. Se obtiene una visión de los parámetros utilizados por BGP para la elección de rutas
7. Aplicando Ingeniería de Trafico con la modificación de los atributos de BGP se logra manipular el trafico saliente de la red Tier 2

4.2 Pruebas

Para validar el diseño de red propuesto utilizando las diferentes instancias del protocolo BGP y también haciendo usos de sus diferentes propiedades como son los reflectores de rutas y la ingeniera de trafico que ofrece mediante la modificación de sus atributos que para esta red se han utilizado Local Preference y MED, se proponen las siguientes pruebas:

1. Realizar pruebas de conectividad entre los equipos y hosts
2. Realizar trazas desde host 1 y 2 a hacia host 3 y viceversa para verificar la ruta que toma el trafico
3. Deshabilitar enlaces al azar para validar la redundancia de la red
4. Deshabilitar R6 o R7 para verificar redundancia en los reflectores
5. Modificar por un valor menor a 100 o deshabilitar el route map del local preference para validar la ruta que toma el trafico sin el valor asignado
6. Intercambiar los valores o deshabilitar el route map del atributo MED para validar la ruta que toma el trafico sin el valor asignado

4.3 Resultados de las pruebas realizadas

1. La red presenta conectividad completa entre todos los equipos y hosts
2. La ruta que toma el trafico en las pruebas es por el enlace que hay entre R10 y R12
3. La red presenta redundancia
4. La red presenta redundancia en el diseño de reflectores
5. El trafico de los hosts 1 y 2 hacia host 3 cambia de enlace de salida de la red Tier 2 y ahora toman la ruta por el enlace entre R9 y R11
6. El trafico de host 3 hacia 1 y 2 cambia de enlace de salida de la red Tier 1 y toma la ruta por el enlace entre R9 y R11

5. Ejercicio propuesto para alumnos de la UPM

La elaboración de estas practicas se realizo en base a los ejercicios impartidos en la UPM para la clases de grado referentes al protocolo OSPF, de manera que se ha utilizado un formato similar para seguir con la misma línea de trabajo que se ha utilizado con los alumnos.

El ejercicio consiste en el estudio y comprensión del funcionamiento del protocolo BGP y sus características sobre un escenario IP emulado mediante la virtualización.

El escenario inicial estará compuesto por 15 maquinas virtuales con sistema operativo Linux. Tres de las maquinas utilizadas en la red tienen la finalidad de trabajar como sistemas finales (H1, H2 y H3) y las 12 maquinas restantes trabajaran como routers (R1, R2, R3, R4, R5, R6, R7, R8, R9, R10, R11 y R12). En las maquinas virtuales que trabajan como routers se utilizara el software "quagga" (www.quagga.net) el cual implementa diversos protocolos de encaminamiento dinamico para redes IP, entre ellos BGP.

A través de la interacción con los comandos de gestión, las herramientas ping y traceroute se realizarán una serie de pruebas que permitirán observar el funcionamiento real de BGP conforme se vaya solicitando a los alumnos la configuración en turno o modificaciones en la red. Con los comandos de configuración de BGP, se configurará en el escenario de red un segundo reflector de rutas el cual tiene la finalidad de trabajar como reflector secundario y brindara conexión a las diferentes redes ya existentes, posteriormente después de realizar los análisis necesarios con los comandos de gestión se configuraran parámetros de Ingeniería de Trafico para manipular la ruta que toma el trafico entrante y saliente de la red y así poder analizar su comportamiento y sus parámetros. Durante la realización del trabajo, se obtendrá la información sobre la red necesaria para permitir contestar a las preguntas que se plantean en el formulario de entrega.

La realización del ejercicio se podrá realizar desde un ordenador propio ya que la red implementada cuenta con todos los parámetros y elementos para realizar el ejercicio. En el primer caso, se necesitarán unos 9 GB libres en disco duro. El trabajo se realizará utilizando VirtualBox, un software de virtualización gratuito disponible para Linux, Windows o Mac OSX. Esto permitirá arrancar una máquina virtual Ubuntu con todo el software necesario. Esta alternativa facilita la realización del trabajo, ya que es posible guardar el estado de la máquina virtual y continuar trabajando en el mismo estado que se dejó.

5.1 Arranque del escenario.

Para comenzar la práctica debe arrancar el escenario mediante los pasos siguientes:

1. Si utiliza ordenador propio, siga los siguientes pasos:

- Descargue e instale VirtualBox desde http:///www.virtualbox.org. Debe instalar además el "VM VirtualBox Extension Pack" disponible también en la página de descargas.

- Descargue la máquina virtual a su ordenador desde el enlace disponible en el moodle de RDOR.

- Arranque VirtualBox y acceda al menú "Archivo->Importar servicio virtualizado", seleccione el fichero de la máquina virtual y a continuación dele al botón "Importar".

Una vez finalizada la importación, seleccione la máquina virtual y pulse el botón "Iniciar" para arrancarla

2.Haga doble click sobre el fichero rdor-XXX.tar.

3. Para arrancar y detener el escenario se utilizaran los siguientes comandos desde la terminal accediendo a las carpetas en donde se encuentra el archivo del escenario

sudo vnx –f bgptest.xml -v –t (arrancar)

sudo vnx –f bgptest.xml -v –P (detener)

Una vez haya arrancado el escenario (tarda entre 80 y 200 seg. dependiendo del ordenador), debe ver en pantalla las consolas de todos los sistemas que componen el escenario: doce routers (R1, R2, R3, R4, R5, R6, R7, R8, R9, R10, R11 y R12) y tres sistemas finales (H1, H2 y H3).

El acceso a los sistemas se puede realizar a través de su consola utilizando como

usuario “root” y como clave “xxxx”. Adicionalmente, se puede acceder mediante un terminal (“Aplicaciones|Accesorios|Terminal”) y la ejecución de un slogin a la máquina deseada. Por ejemplo: “slogin R1 –l root” le dará acceso al router R1.

El acceso a la configuración de los routers se realiza ejecutando el comando vtysh que nos proporciona una consola con comandos similares a los de los routers CISCO.

Los siguientes comandos de quagga (a ejecutar dentro de vtysh) le serán de utilidad para la realización de la práctica:

- **show ip route**. Muestra las tablas de encaminamiento de un router.
- **show ip bgp neighbor**. Muestra los vecinos bgp de un router.
- **show ip bgp summary**. Muestra el resumen de los estatus de los vecinos BGP
- **show ip bgp (network/prefix)**. Muestra los parametros de una ruta aprendida por BGP
- **show interface**. Muestra los interfaces de red del router.
- **show ip bgp**. Muestra las rutas aprendidas por BGP
- **ping y traceroute**. Acceso desde vtysh a los comandos ping y traceroute estándar.

Otros comandos de interés que se pueden ejecutar en las máquinas virtuales (desde fuera de vtysh):

- **ifconfig (o “ip address”)**. Muestra los interfaces de red de un sistema. Nota: ignore los interfaces “eth0” de todos los sistemas (se utilizan internamente para la gestión de los escenarios virtuales).
- **ping y traceroute**. Se recomienda usar la opción “-n” de traceroute para evitar que intente buscar la correspondencia entre dirección IP y nombre de máquina.

5.2 BGP - Pasos a seguir

El ejercicio va a consistir en configurar un segundo reflector de rutas que trabajara como equipo secundario para que al simular una falla en el reflector de rutas primario este provea redundancia, posteriormente se configuraran los parámetros de ingeniera de trafico en el borde de la red que conecta el AS1 con el AS10 en los equipos R9 y R10 .Se realizarán también pruebas que permitan observar y analizar el comportamiento del trafico y los parámetros que presentan las rutas propagadas por BGP así como los mensajes enviados y la reconfiguración de la red en caso de caída de un enlace.

5.3 Análisis y configuración de la practica

Realizar los puntos solicitados utilizando las Tablas 6, 7 y 8

1. Realizar traceroute desde H1 y H2 hacia H3 y viceversa. Que ruta toma el trafico para llegar a su destino?
2. Aplicar R3, R6 y 11 los comandos de gestión que se encuentran dentro de la Tabla de Gestión para analizar y describir la información que arrojan
3. Realizar la siguiente configuración con los comandos que contiene la Tabla de Configuración y la tabla de interfaces abajo insertadas
4. Configurar R7 como reflector secundario declarando como clientes a R3, R4, R5, R8, R9 y R10 dentro del mismo AS.
5. Asignar a R7 el cluster id 2.2.2.2
6. Configurar un enlace iBGP entre R7 y R6.
7. Configurar para cada peer con el que conecta R7 el atributo de Next-hop por medio de los mapas de ruta.
8. Repetir paso 1 y 2.
9. Deshabilitar enlaces y realizar pruebas de traceroute entre H1, H2 y H3 para comprobar redundancia
10. Deshabilitar en R6 el protocolo de ruteo BGP con el comando “no bgp route (AS)”
11. Realizar traceroute desde H1 y H2 hacia H3 y viceversa. Que ruta toma el trafico para llegar a su destino?
12. Modificar el atributo Local Preference en R10 para el trafico de entrada que proviene de R12 asignando un valor de 500 (Tabla de Configuración)
13. Configurar MED con un valor de 50 en R10 para el trafico de salida a R12 (Tabla de Configuración)
14. Configurar MED con un valor de 200 en R9 para el trafico de salida a R11 (Tabla de Configuración)
15. Repetir paso 1 y 2 en R3, R7 y R11

Show ip route	Rutas y como fueron aprendidas
Show ip bgp neighbors	Vecinos, IP y AS
Show ip bgp summary	Vecinos, versión bgp, AS, estatus de sesión bgp y tipos de mensajes enviados y recibidos
Show ip bgp (network/prefix)	Originator ID y Cluster ID
Shoqw ip bgp	Rutas, next-hop, metric, local preference, weigth y path

Tabla 6: Comandos de gestión

Configure terminal
Router bgp (AS)
Bgp cluster-id (x.x.x.x)
Neighbor (Peer) remote-as (AS)
Neighbor (peer) route-reflector-client
Neighbor (peer) route-map (name route-map) in/out
Route-map (name) permit (number sequence)
Set (atribute) (value)
Set ip next-hop (peer)

Tabla 7: Comandos de configuración

Inteface	Direccion IP	Vecino
eth1	10.3.1.22/30	R4
eth2	10.3.1.14/30	R3
eth3	10.3.1.38/30	R6
eth4	10.3.1.41/30	R9
eth5	10.3.1.45/30	R10
eth6	10.3.1.49/30	R8
eth7	10.3.1.54/30	R5

Tabla 8: Interfaces R7

5.4 Formulario

1. ¿Que ruta toma el traceroute entre hosts en el punto 1?
2. Describa la información que enlista cada uno de los comandos del punto 2
3. ¿Que información nueva aparecer después de configurar el punto 3 y repetir el punto 1 y 2?
4. ¿Al deshabilitar los enlaces encontramos redundancia?
5. Después de deshabilitar BGP en R6 y repetir el punto 1 y 2 que ruta toma el trafico ¿Que información ha desaparecido?
6. Después de habilitar el Local Preference y MED ¿en que equipos se presenta el cambio de valores de los atributos?

6. Conclusiones y trabajos futuros

6.1 Conclusiones

Como se ha dicho con anterioridad, las redes de comunicaciones tiene el propósito de llevar paquetes de datos los cuales contienen información generada por los millones de usuarios que se conectan al internet día con día. El crecimiento de usuarios es muy agresivo ya que continuamente se multiplican los dispositivos que tienen la capacidad de conectarse a la red, esto conlleva que haya una explosión en el numero de identificadores llamados direcciones IP las cuales necesitan para conectarse y ser localizados, de manera que el numero de tablas de enrutamiento existentes en el mundo es y grande . Los protocolos de enrutamiento tienen la finalidad de proveer

comunicación en la red, administrando las tablas de enrutamiento y eligiendo las mejores rutas disponibles. BGP es el protocolo encargado de brindar administrar las direcciones IP y brindar comunicaciones dentro de internet, ya se basa en Sistemas Autónomos para realizar el enrutamiento. Además de brindar comunicación también tiene la capacidad de ofrecer ingeniería de trafico con lo cual aporta aun mayor granularidad al control del trafico pudiendo adaptarlo a las necesidades de los clientes o usuario final. Este protocolo tiene tal flexibilidad que puede trabajar en conjunto con otros protocolos de enrutamiento interno de manera que es utilizado dentro de las redes privadas junto con otros haciendo uso de las herramientas que ofrece para el control de trafico y administración de las tablas de enrutamiento

En este documento se ha presentado un estudio de todas sus capacidades y se ha implementado mediante virtualización un diseño de red utilizando el protocolo BGP con la cual se logro visualizar de manera muy clara sus capacidades y de que manera opera llegando a una comprensión completa del mismo, tanto en lo teórico como en lo practico. Al implementar una red con BGP se puede observar bien de que manera se comporta el trafico y como trabajan los atributos del protocolo para la elección de las rutas, ya que también al configurar la red se tuvo la necesidad de realizar troubleshooting y esto obliga a estudiar y tratar de entender aun mas el funcionamiento del protocolo.

Con la red Implementada se realizo la elaboración de practicas para el alumnado de la Universidad Politécnica de Madrid con las cuales se podrán impartir practicas de laboratorio para la comprensión teórica y practica de las características y capacidades del protocolo de enrutamiento BGP solicitando la configuración de los equipos dependiendo de la función que realicen dentro de la red. Con la realización de estas practicas y los ejercicios propuestos se obtienen una visión de la operación del protocolo en las redes de datos.

6.2 Trabajos Futuros

El trabajo desarrollado en este documento tiene una línea de investigación muy amplia ya que la tecnología avanza día con día de manera muy rápida y los escenario s que puede presentar una red pueden varias de acuerdo a las necesidades de los usuarios, de manera que algunos puntos para las siguientes líneas de trabajo podrían ser los siguientes

1. Considerar el cambio de diseño de red para identificar la necesidad de implementar un Protocolo de Gateway Interior en paralelo con BGP
2. Implementar BGP junto con OSPF para analizar como se comportan los protocolos por medio de la redistribución de rutas entre ellos
3. Aplicar modificación de otros atributos BGP para realizar ingeniera de trafico como Weight y AS-path
4. Implementar comunidades de BGP para analizar el comportamiento asociándolas con los diferentes atributos de BGP
5. Agregar segmentos de red a la red para poder utilizar las diferentes técnicas de filtrados de rutas como Prefix List, Distribition Lis y Filter List y visualizar de que manera se realiza el filtrado de rutas entre carries cuando se pretende hacer peering
6. Levantar sesiones BGP por medio de interfaces virtuales y la utilización de algun IGP para verificar la estabilidad de las sesiones BGP en caso de caídas de enlaces
7. Implementación de MPLS sobre BGP

En general con la red implementada se pueden realizar los punto 3, 4, 5 y 6 por lo que no habría necesidad de cambiar el diseño de red ni agregar algun otro tipo de demoni para poder aplicar configuraciones, ya que todos los cabios los soporta el demonio de BGP. Para la aplicación del punto 1, 2 y 7 es necesario agregar los demonios de los protocolos que se quieren implementar y se recomendaría cambiar el diseño de red para visualizar de mejor manera que ventajas tiene la aplicación de estos protocolos.

Bibliografía

[1] Beijnum, Iljitsch van. *BGP.* Sebastopol, CA: O'Reilly & Associates, Inc, 2002.

[2] Ishiguro, Kunihiro. *Quagga Routing Suite.* 2009. http://www.nongnu.org/quagga/ (último acceso: 2012).

[3] Madrid, Universidad Politecnica de. *Virtual Networks over Linux.* 2012. http://web.dit.upm.es/vnxwiki/index.php/Wikisite (último acceso: 2012).

[4] White, Russ, Danny McPherson, y Sangli Srihari. *Practical BGP.* Boston, MA: Pearson Education, Inc., 2005.