PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

MAESTRÍA EN REDES DE COMUNICACIONES

PERFIL DEL TRABAJO PREVIO A LA OBTENCION DEL TÍTULO DE:

MASTER EN REDES DE COMUNICACIONES

TEMA:

"DISEÑO E IMPLEMENTACION A NIVEL DE LABORATORIO DE UNA RED MULTI-PROTOCOLO REDUNDANTE CON ALTA DISPONIBILIDAD DE ENLACES A NIVEL DE LAN, WAN, FIREWALL. CASO DE ESTUDIO: EMPRESA MIKRODOM S.A."

WLADIMIR EDISON MORALES OCAÑA

Quito – 2016

AUTORÍA

Yo, ***WLADIMIR EDISON MORALES OCAÑA***, portador de la cédula de ciudadanía No. ***171730977-5***, declaro bajo juramento que la presente investigación es de total responsabilidad del autor, y que se he respetado las diferentes fuentes de información realizando las citas correspondientes. Esta investigación no contiene plagio alguno y es resultado de un trabajo serio desarrollado en su totalidad por mi persona.

_____

Wladimir Edison Morales Ocaña

CI: 171730977-5

Contenido

Figuras

Tablas

Ecuaciones

1. Introducción

El presente trabajo de titulación se enfoca en el diseño de una topología de red, en la cual convergen múltiples protocolos de enrutamiento dinámico avanzado para simular una conexión ISP.

El presente proyecto hace énfasis en los principales aspectos que demandan las actuales redes de datos:

1. *Conectividad avanzada*
2. *Redundancia*

Para la realización de este trabajo de grado, se ha tenido en consideración el uso de las principales tecnologías y protocolos de enrutamiento avanzado para redes escalables, y el uso de múltiples soluciones para ofrecer mecanismos de redundancia tanto en la red LAN, WAN y Firewall. Todo esto con el fin de simular en la medida de lo posible una topología de red real en un ambiente de laboratorio.

Se ha hecho énfasis en la convergencia de los principales protocolos de enrutamiento dinámico que se utilizan en Sistemas Autónomos los cuales están en la capacidad de manejar tablas de enrutamiento muy grande como las que se tiene en la actualidad.

La disponibilidad y balaceo de carga a nivel de LAN estará controlada mediante el protocolo dinámico GLBP, de esta forma al caer el enlace principal hacia el Router Master AVG, se conmutará hacia el router AVF haciendo que no se vea afectado el servicio propuesto en el presente caso de estudio además de brindar compartición de carga.

Las políticas de enrutamiento de tráfico y alta disponibilidad a nivel de WAN estarán a cargo de las capabilities MED y Local Preference y el toolkit del protocolo de internet BGP en sesiones eBGP, para este fin se aplicará PBR con el objetivo de manipular el tráfico de upstream según el destino hacia el AS vecino.

Para fines demostrativos de BGP, se manipulará el tráfico de upstream generado en un Sistema Autónomo para escoger como enlace favorito según sea la red de destino deseado. Así mismo al haber una falla con los 2 enlaces hacia el ISP principal, todo el tráfico conmutará hacia ISP de backup de forma automática, todo esto para ofrecer alta disponibilidad en el servicio.

Todo esto será posible gracias a una topología de 23 equipos de networking, entre routers, switches y firewalls en un ambiente de laboratorio con equipos físicos reales.

2. Justificación

La aparición de internet como un mecanismo de comunicación masivo, hace que miles de personas se conecten a esta red mundial la cual es publica, lo que conlleva a que el usuario se encuentre expuesto a un sin número de problemas y caídas de enlaces. Los routers de los proveedores de servicios (ISPs) son los encargados de enrutar y direccionar los paquetes de datos seleccionando el mejor camino desde un nodo local hacia un destino remoto, esto hace que por medio de estos dispositivos atraviesen y fluya toda la información que intercambian las redes de datos.

A finales de la década de 1980 surge la importancia y el interés sobre los protocolos de enrutamiento dinámico en redes tipo escalables; así es como BGP se desarrolló, como un protocolo EGP para antiguos ambientes centralizados de internet (ARPANET), pasando a ser parte de un ambiente distribuido capaz de implementar políticas de enrutamiento, direccionar paquetes de datos e intercambiar información que provienen de diversos protocolos de enrutamiento internos como EIGRP, IGRP, OSPF, IS-IS los cuales trabajan dentro de sistemas autónomos.

Una vez plantado BGP como el protocolo de enrutamiento que usan los Proveedores de Servicio de Internet (ISPs) para ofrecer a los usuarios conexión a internet, se ha producido un crecimiento acelerado de usuarios en la red, altos índices de inseguridades virtuales, la necesidad de incorporar sistemas unificados de comunicaciones, y la interconexión de redes de comunicaciones en todo el mundo mediante el Backbone de internet, han llevado a ser los temas de interés para todas las personas y empresas que hacen uso de esta gran red abierta como Internet.

El uso de plataformas convergentes, donde fluye todo tipo de datos por el medio (audio, datos, video) hace necesario el aprovechamiento al máximo del recurso de internet y lograr entre otras cosas la transmisión de voz digitalizada por sobre cualquier tipo de medio que esté disponible (Fibra óptica, Cobre, Wireless).

La redundancia a nivel de LAN con el uso del protocolo GLBP, provee al sistema un mecanismo robusto y automático de selección de múltiples gateways simultáneos en caso de fallas, lo cual implica tener load-sharing de paquetes y diversos caminos para solucionar peticiones ARP usando tracking de objetos.

El toolkit de BGP permitirá realizar tareas de manipulación de tráfico de up y downstream ante fallas y pérdida de enlaces hacia los ISP's (Service Prividers) mediante Multi-homing tomando en consideración herramientas como: Prefix-lists, Filter-lists y Route-maps. La implementación

de políticas de enrutamiento a nivel de AS en caso de fallas, se las realiza por medio de atributos de BGP como: MED y Local Preference.

Una de las características principales de la topología es tener alta capacidad de escalabilidad gracias al uso de Route-Reflectors en cada Sistema Autónomo, así como de redundancia por la implementación de Multi-Homing a nivel de BGP. La seguridad no se encuentra de lado ya que se aplica bogons e identificación de AS's de Tránsito.

El uso de Firewalls ASA 5520 en cada extremo de la topología de red, asegura alta disponibilidad en sus enlaces en casos de caída o flapeo mediante interfaces redundantes (Active/Standby), así como rutas estáticas confiables con el uso de tracking de objetos y SLA.

Bajo estas premisas es pertinente considerar que:

1. *Al tener sistemas que interconectan redes remotas, las usuarios envían correos electrónicos, archivos, ocupan mensajería instantánea, hacen llamadas de voz por internet, haciendo que la información se convierta en el recurso más valioso para una empresa.*
2. *Los paquetes de datos viajan por la red pública, desde un nodo de acceso origen a un nodo de acceso destino por medio de un conjunto de nodos intermedios.*
3. *Las redes privadas pueden llegar a tener una envergadura considerable, haciendo que manejen sus propios protocolos de enrutamiento internos.*
4. *Una infraestructura de red debe balancear tanto la distribución óptima del tráfico de red como los mecanismos de control de acceso.*

Hacen que sea de suma importancia la convergencia de múltiples protocolos de enrutamiento avanzados para asegurar la conectividad, alta disponibilidad, integridad, y escalabilidad que las redes de datos actuales necesitan.

3. Antecedentes

En la actualidad el uso de recursos que se ofrece en Internet ha crecido de forma exponencial en los últimos años, dando como resultado que la mayoría de aplicaciones en el mercado consuman alto porcentaje de ancho de banda, ya sea por manejo de datos, streaming de video, telefonía IP y aplicaciones que demandan alto tráfico en tiempo real.

La marcha para el mundo de las redes actuales iniciaron en la década de 1980, cuando las empresas de networking mostraron interés en desarrollar dispositivos los cuales eran capaces de unir redes remotas. Lamentablemente siendo su crecimiento de forma desordenada e incompatible entre otras marcas y vendors, hicieron que no sea posible la inter-operatividad entre redes debido al uso de múltiples y diversas plataformas o protocolos propietarios.

A partir de esto, la entidad ISO realizó un protocolo de comunicaciones que posteriormente se convirtió en un modelo de referencia estándar, un modelo desarrollado en el metalenguaje ASN.1 el cual hace que el nodo transmisor tenga el control sobre la máquina de estados finitos del receptor y viceversa.

Por lo mencionado anteriormente existen en la actualidad muchas empresas que todavía tienen sus redes y recursos dispersos en su misma organización, debido a no tener los mecanismos suficientes para integrar y brindar convergencia y alta disponibilidad que garanticen la continuidad del negocio y de todas las funciones operativas que esto implica.

Uno de los problemas a enfrentarse en la actualidad es la integración de múltiples protocolos de enrutamiento dentro de un mismo Sistema Autónomo (AS), y es que por muchas razones, las empresas deciden manejar diversos protocolos IGP ya sea por cuestiones técnicas, requerimientos o presupuesto. Todos los protocolos a ser usados requieren intercambiar información de manera óptima, económica y lo más rápida posible independientemente del protocolo que se utilice.

El tráfico de diferentes aplicaciones de red empresariales como: Correo electrónico, llamadas IP, páginas web, bases de datos y sistemas de gestión deben pasan necesariamente por enlaces LAN, WAN o de cualquier otro tipo. Por lo que si hay intermitencia en los enlaces, excesivo tráfico e interrupciones del servicio la red y aplicaciones, la red debe estar en la capacidad de buscar nuevos caminos, a pesar de manejar distintos protocolos de comunicaciones

Para alcanzar gran escalabilidad, eficiencia en el direccionamiento IP, funcionalidad para topologías grandes y convergentes, se plantea como referencia la presente investigación la cual, mediante la ejecución y convergencia de múltiples protocolos de enrutamiento avanzado, y alta disponibilidad, hacen posible la sostenibilidad de una infraestructura de este tipo.

Como ejes fundamentales del presente caso de estudio se tiene:

1. *Enrutamiento avanzado*
2. *Alta redundancia y disponibilidad*

Tomando en cuenta que existen varios sistemas autónomos y cada uno tiene ciertas características de tráfico de red, se optó por usar EIGRP por ser un tipo de protocolo Classless, gran capacidad de escalabilidad, eficiencia en entornos IPV4 e IPV6, envío de actualizaciones confiables, además de soportar balanceo de carga desigual. OSPF ofrece a la presente topología convergencia rápida, optimización del ancho de banda, uso de multicast para envío de actualizaciones incrementales y pudiendo manejar virtual-links para áreas discontinuas del backbone de la red. Por otro lado IS-IS es el protocolo estándar favorito cuando se tiene decenas y miles de nodos multi-vendors en la red.

Se usa en el desarrollo del presente caso de estudio el protocolo BGP, como mecanismo para intercambiar información libre de bucles entre sistemas autónomos, así como para definir control de rutas, y políticas de enrutamiento basadas en seguridad y costo. Finalmente para afinar el diseño de conectividad entre sistemas autónomos (AS) se usará el proceso de redistribución de rutas y compartición de carga.

Con el objetivo de implementar políticas de acceso e inspección de tráfico en sentido entrante y saliente a la red, se recomienda que los servicios de una empresa se encuentren dentro de una zona segura desmilitarizada llamada DMZ, ubicada entre la red interna de una organización y la red externa.

Con el objetivo de implementar alta disponibilidad a nivel de ASA, se propone 2 mecanismos para conseguir este propósito, uno por cada Sistema Autónomo:

- *Alta disponibilidad con interfaces redundantes*
- *Rutas estáticas confiables o "Reliable static route"*

1. *Mediante las pruebas respectivas, se tendrá como alcance verificar el emparejamiento de dos interfaces físicas (una en modo activa y otra en modo Standby) como mecanismo failover. A modo que, cuando el enlace principal falle, la interfaz Standby tome el rol de activa y permita el flujo normal de tráfico, disminuyendo de esta manera tiempos fuera de servicio y aumentando la fiabilidad de la red.*

Por otro lado, se utilizará como mecanismo de alta disponibilidad la configuración de SLA (Service-Level Agreement), atando una ruta estática confiable a un objeto para realizar tracking. De esta forma se verificará continuamente el estado del objeto para tomar la decisión de conmutación de enlace e inserción de una nueva ruta según su estado en la tabla de enrutamiento.

4. Objetivos

Objetivo General:

Diseñar e implementar a nivel de laboratorio una red multi-protocolo redundante con alta disponibilidad de enlaces a nivel de LAN, WAN, FIREWALL en la empresa MIKRODOM S.A.

Objetivos Específicos:

1. *Comprobar la conectividad de la topología e integración de diferentes protocolos de enrutamiento dinámico avanzado mediante redistribución de rutas y toolkit de cada protocolo.*

2. *Implementar una topología redundante a nivel de LAN con el uso del protocolo GLBP, a nivel de WAN mediante el toolkit de BGP y Multi-homing, así como a nivel de Firewall mediante enlaces redundantes y tracking de objetos para tener alta disponibilidad.*

3. *Monitorear y generar alarmas de tráfico vía correo electrónico y mensajes de texto (SMS) mediante el uso de una plataforma basada en Open Source y un circuito electrónico usando microcontroladores PIC.*

5. Conectividad de la topología e integración de diferentes protocolos de enrutamiento dinámico avanzado mediante redistribución de rutas y toolkit de cada protocolo.

5.1. Esquema de direccionamiento

El presente caso de estudio tiene una arquitectura de laboratorio que simula dos Sistemas Autónomos Públicos de 2 bytes, los cuales tienen conexión entre sí a través de dos diferentes Proveedores de Servicio (ISPs). Para la realización del presente estudio, los Sistemas Autónomos son organizaciones Multi-Homed, es decir cuentan con al menos dos enlaces activos a Internet sin que dependa uno del otro.

El Sistema Autónomo Público 100 representa la estructura de red de la Empresa Mikrodom S.A en Ecuador, donde tiene su matriz y parte de sucursales a nivel nacional:

- *Guayaquil (GYE)*
- *Quito (UIO)*
- *Cuenca (CCA)*
- *Ambato (AMB)*
- *Loja (LJA)*
- *Imbabura (IMB)*

A pesar de la no utilización de Frame Relay en la actualidad, con el fin de proporcionar conectividad y conexión a través de la red pública entre usuarios del AS100 y demostrar la facilidad de convergencia de varios protocolos de enrutamiento dinámico avanzado en la red, se implementará una nube de este tipo.

Al hacer énfasis en este capítulo sobre la conectividad entre Sistemas Autónomos, es de suma importancia mantener un eficiente esquema de direccionamiento IP con el fin de maximizar la usabilidad IP dentro de la topología, así como la posibilidad de minimizar tablas de enrutamiento mediante el uso de sumarización con distintos protocolos de enrutamiento.

Con el fin de aprovechar con eficiencia el uso de direccionamiento IP y aumentar la cantidad de hosts que podrán conectarse a Internet e intranet en la topología, se opta por un esquema de máscara de red de longitud variable (VLSM) para permitir menor desperdicio en el direccionamiento IP. Esto se logra por medio de la toma de bits prestados de la máscara de subred permitiendo así una mejor distribución entre los host que integran la subred. Hay que considerar que no todos los protocolos de enrutamiento soportan el uso de VLSM, por lo que en el presente trabajo de titulación se utilizarán protocolos que soporten la opción de permitir redes con una diferente máscara de subred que las usadas por defecto en redes Classfull.

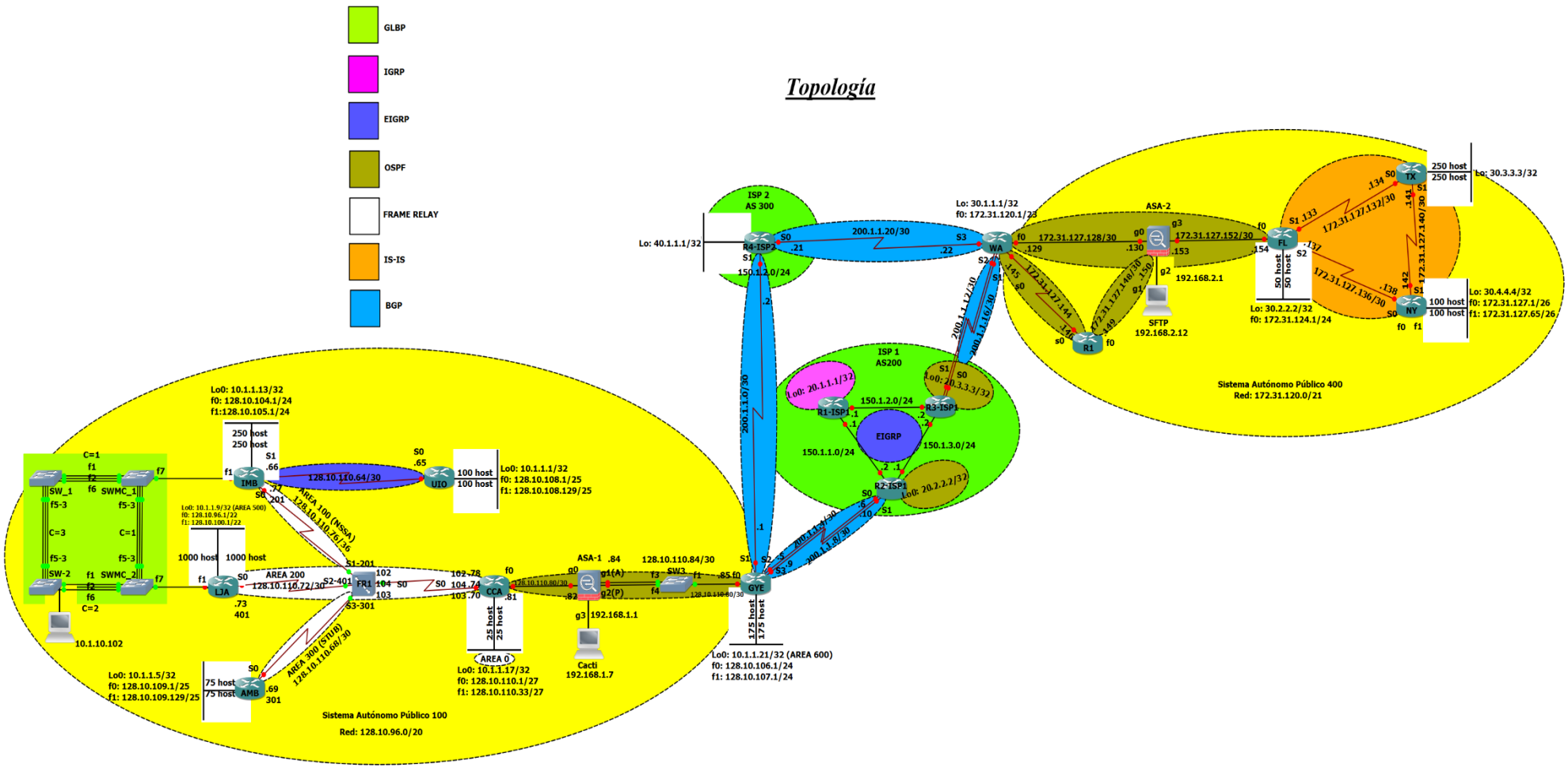


Figura 1: Topología de red.

Realizado por: *Morales, W. 2016.*

Requerimientos - Direccionamiento AS 100

Sucursal	Fastethernet 0/1	Fastethernet 0/2	Total
	hosts	hosts	hosts
LOJA	1000	1000	2000
IMBABURA	250	250	500
GUAYAQUIL	175	175	350
QUITO	100	100	200
AMBATO	75	75	150
CUENCA	50	50	100
Total			3300

Figura 2: *Cálculo de subredes*

Realizado por: *Morales, W. 2016.*

Calculo de Subredes AS100

Datos:

Red: *128.10.X.0/20*

Subred: *6*

X*=96*

Total: *3300 hosts;* $\boldsymbol{n = 12}$

Direccionamiento IP - AS 100		
Red	128.10.96.0/20	255.255.240.0
Broadcast	128.10.111.255/20	

Figura 3: Cálculo de subredes AS 100

Realizado por: *Morales, W. 2016.*

LJA – Fa 0/0 (1000 hosts):

$$\boldsymbol{Host\ válidos = 2^n - 2\ ;}$$

$$\boldsymbol{n = 10}$$

$$\boldsymbol{Host\ válidos = 1022}$$

LJA	Fastethernet 0/0	Máscara
Subred	128.10.96.0/22	255.255.252.0
Gateway	128.10.96.1/22	
Primera valida	128.10.96.2/22	
Ultima valida	128.10.96.254/22	
Broadcast	128.10.99.255/22	

Figura 4: Cálculo de subredes AS 100-LJA

Realizado por: *Morales, W. 2016.*

LJA – Fa 0/1 (1000 hosts):

$$\boldsymbol{Host\ válidos = 2^n - 2\ ;}$$

$$\boldsymbol{n = 10}$$

$$\boldsymbol{Host\ válidos = 1022}$$

LJA	Fastethernet 0/1	Máscara
Subred	128.10.100.0/22	255.255.252.0
Gateway	128.10.100.1/22	
Primera valida	128.10.100.2/22	
Ultima valida	128.10.100.254/22	
Broadcast	128.10.100.255/22	

Figura 5: Cálculo de subredes AS 100-LJA

Realizado por: *Morales, W. 2016.*

IMB – Fa 0/0 (250 hosts):

$$\boldsymbol{Host\ válidos = 2^n - 2\ ;}$$

$$\boldsymbol{n = 8}$$

$$\boldsymbol{Host\ válidos = 254}$$

IMB	Fastethernet 0/0	Máscara
Subred	128.10.104.0/24	255.255.255.0
Gateway	128.10.104.1/24	
Primera valida	128.10.104.2/24	
Ultima valida	128.10.104.254/24	
Broadcast	128.10.104.255/24	

Figura 6: Cálculo de subredes AS 100-IMB.

Realizado por: *Morales, W. 2016.*

IMB – Fa 0/1 (250 hosts):

$$\boldsymbol{Host\ válidos = 2^n - 2\ ;}$$

$$\boldsymbol{n = 8}$$

$$\boldsymbol{Host\ válidos = 254}$$

IMB	Fastethernet 0/1	Máscara
Subred	128.10.105.0/24	255.255.255.0
Gateway	128.10.105.1/24	
Primera valida	128.10.105.2/24	
Ultima valida	128.10.105.254/24	
Broadcast	128.10.105.255/24	

Figura 7: Cálculo de subredes AS 100-IMB.

Realizado por: *Morales, W. 2016.*

GYE – Fa 0/0 (175 hosts):

$$\boldsymbol{Host\ válidos = 2^n - 2\ ;}$$

$$\boldsymbol{n = 8}$$

$$\boldsymbol{Host\ válidos = 254}$$

GYE	Fastethernet 0/0	Máscara
Subred	128.10.106.0/24	255.255.255.0
Gateway	128.10.106.1/24	
Primera valida	128.10.106.2/24	
Ultima valida	128.10.106.254/24	
Broadcast	128.10.106.255/24	

Figura 8: Cálculo de subredes AS 100-GYE.

Realizado por: *Morales, W. 2016.*

GYE – Fa 0/1 (175 hosts):

$$\boldsymbol{Host\ válidos = 2^n - 2\ ;}$$

$$\boldsymbol{n = 8}$$

$$\boldsymbol{Host\ válidos = 254}$$

GYE	Fastethernet 0/1	Máscara
Subred	128.10.107.0/24	255.255.255.0
Gateway	128.10.107.1/24	
Primera valida	128.10.107.2/24	
Ultima valida	128.10.107.254/24	
Broadcast	128.10.107.255/24	

Figura 9 Cálculo de subredes AS 100-GYE.

Realizado por: *Morales, W. 2016.*

UIO – Fa 0/0 (100 hosts):

$$\boldsymbol{Host\ válidos = 2^n - 2\ ;}$$

$$\boldsymbol{n = 7}$$

$$\boldsymbol{Host\ válidos = 126}$$

UIO	Fastethernet 0/0	Máscara
Subred	128.10.108.0/25	255.255.255.128
Gateway	128.10.108.1/25	
Primera valida	128.10.108.2/25	
Ultima valida	128.10.108.126/25	
Broadcast	128.10.108.127/25	

Figura 10 Cálculo de subredes AS 100-UIO

Realizado por: *Morales, W. 2016.*

UIO – Fa 0/1 (100 hosts):

$$\boldsymbol{Host\ válidos = 2^n - 2\ ;}$$

$$\boldsymbol{n = 7}$$

$$\boldsymbol{Host\ válidos = 126}$$

UIO	Fastethernet 0/1	Máscara
Subred	128.10.108.128/25	255.255.255.128
Gateway	128.10.108.129/25	
Primera valida	128.10.108.130/25	
Ultima valida	128.10.108.254/25	
Broadcast	128.10.108.255/25	

Figura 11 Cálculo de subredes AS 100-UIO

Realizado por: *Morales, W. 2016.*

AMB – Fa 0/0 (75 hosts):

$$\boldsymbol{Host\ válidos = 2^n - 2\ ;}$$

$$\boldsymbol{n = 7}$$

$$\boldsymbol{Host\ válidos = 126}$$

AMB	Fastethernet 0/0	Máscara
Subred	128.10.109.0/25	255.255.255.128
Gateway	128.10.109.1/25	
Primera valida	128.10.109.2/25	
Ultima valida	128.10.109.126/25	
Broadcast	128.10.109.127/25	

Figura 12 Cálculo de subredes AS 100-AMB

Realizado por: *Morales, W. 2016.*

AMB – Fa 0/1 (75 hosts):

$$\boldsymbol{Host\ válidos = 2^n - 2\ ;}$$

$$\boldsymbol{n = 7}$$

$$\boldsymbol{Host\ válidos = 126}$$

AMB	Fastethernet 0/1	Máscara
Subred	128.10.109.128/25	255.255.255.128
Gateway	128.10.109.129/25	
Primera valida	128.10.109.130/25	
Ultima valida	128.10.109.254/25	
Broadcast	128.10.109.255/25	

Figura 13 Cálculo de subredes AS 100-AMB

Realizado por: *Morales, W. 2016.*

CCA – Fa 0/0 (25 hosts):

$$\boldsymbol{Host\ válidos = 2^n - 2\ ;}$$

$$\boldsymbol{n = 5}$$

$$\boldsymbol{Host\ válidos = 30}$$

CCA	Fastethernet 0/0	Máscara
Subred	128.10.110.0/27	255.255.255.224
Gateway	128.10.110.1/27	
Primera valida	128.10.110.2/27	
Ultima valida	128.10.110.30/27	
Broadcast	128.10.110.31/27	

Figura 14 Cálculo de subredes AS 100-CCA.

Realizado por: *Morales, W. 2016.*

CCA – Fa 0/1 (25 hosts):

$$\boldsymbol{Host\ válidos = 2^n - 2\ ;}$$

$$\boldsymbol{n = 5}$$

$$\boldsymbol{Host\ válidos = 30}$$

AMB	Fastethernet 0/1	Máscara
Subred	128.10.110.32/27	255.255.255.224
Gateway	128.10.110.33/27	
Primera valida	128.10.110.34/27	
Ultima valida	128.10.110.62/27	
Broadcast	128.10.110.63/27	

Figura 15 Cálculo de subredes AS 100-CCA.

Realizado por: *Morales, W. 2016.*

Requerimientos - Direccionamiento AS 400

Cantidad de hosts:

Sucursal	Fastethernet 0/1	Fastethernet 0/2	Total
	hosts	hosts	hosts
WA	500	500	1000
CA	100	100	200
FL	250	250	500
NY	50	50	100
Total			1800

Figura 16 Cálculo de subredes AS 400

Realizado por: *Morales, W. 2016.*

Calculo de Subredes AS400

Datos:

Red: *172.31.X.0/21*

Subred: *15*

X*=120*

Total: *1800 hosts;* $\boldsymbol{n = 11}$

Direccionamiento IP - AS 400		
Red	172.31.120.0/21	255.255.248.0
Broadcast	172.30.127.255/21	

Figura 17 Cálculo de subredes AS 400

Realizado por: *Morales, W. 2016.*

WA – Fa 0/0 (500 hosts):

$$\boldsymbol{Host\ válidos = 2^n - 2\ ;}$$

$$\boldsymbol{n = 9}$$

$$\boldsymbol{Host\ válidos = 510}$$

WA	Fastethernet 0/0	Máscara
Subred	172.31.120.0/23	255.255.254.0
Gateway	172.31.120.1/23	
Primera valida	172.31.120.2/23	
Ultima valida	172.31.120.254/23	
Broadcast	172.31.121.255/23	

Figura 18 Cálculo de subredes AS 100-WA

Realizado por: *Morales, W. 2016.*

WA – Fa 0/1 (500 hosts):

$$\boldsymbol{Host\ válidos = 2^n - 2\ ;}$$

$$\boldsymbol{n = 9}$$

$$\boldsymbol{Host\ válidos = 510}$$

WA	Fastethernet 0/1	Máscara
Subred	172.31.122.0/23	255.255.254.0
Gateway	172.31.122.1/23	
Primera valida	172.31.122.2/23	
Ultima valida	172.31.122.254/23	
Broadcast	172.31.122.255/23	

Figura 19 Cálculo de subredes AS 100-WA

Realizado por: *Morales, W. 2016.*

FL – Fa 0/0 (250 hosts):

$$\boldsymbol{Host\ válidos = 2^n - 2\ ;}$$

$$\boldsymbol{n = 8}$$

$$\boldsymbol{Host\ válidos = 254}$$

FL	Fastethernet 0/0	Máscara
Subred	172.31.124.0/24	255.255.255.0
Gateway	172.31.124.1/24	
Primera valida	172.31.124.2/24	
Ultima valida	172.31.124.254/24	
Broadcast	172.31.124.255/24	

Figura 20 Cálculo de subredes AS 400

Realizado por: *Morales, W. 2016.*

FL – Fa 0/1 (250 hosts):

$$\boldsymbol{Host\ válidos = 2^n - 2\ ;}$$

$$\boldsymbol{n = 8}$$

$$\boldsymbol{Host\ válidos = 254}$$

FL	Fastethernet 0/1	Máscara
Subred	172.31.125.0/24	255.255.255.0
Gateway	172.31.125.1/24	
Primera valida	172.31.125.2/24	
Ultima valida	172.31.125.254/24	
Broadcast	172.31.125.255/24	

Figura 21 Cálculo de subredes AS 100-FL.

Realizado por: *Morales, W. 2016.*

CA – Fa 0/0 (100 hosts):

$$\boldsymbol{Host\ válidos = 2^n - 2\ ;}$$

$$\boldsymbol{n = 7}$$

$$\boldsymbol{Host\ válidos = 126}$$

CA	Fastethernet 0/0	Máscara
Subred	172.31.126.0/25	255.255.255.128
Gateway	172.31.126.1/25	
Primera valida	172.31.126.2/25	
Ultima valida	172.31.126.126/25	
Broadcast	172.31.126.127/25	

Figura 22 Cálculo de subredes AS 100-CA.

Realizado por: *Morales, W. 2016.*

CA – Fa 0/1 (100 hosts):

$$\boldsymbol{Host\ válidos = 2^n - 2\ ;}$$

$$\boldsymbol{n = 7}$$

$$\boldsymbol{Host\ válidos = 126}$$

CA	Fastethernet 0/1	Máscara
Subred	172.31.126.128/25	255.255.255.128
Gateway	172.31.126.129/25	
Primera valida	172.31.126.130/25	
Ultima valida	172.31.126.254/25	
Broadcast	172.31.126.255/25	

Figura 23 Cálculo de subredes AS 100-CA.

Realizado por: *Morales, W. 2016.*

NY – Fa 0/0 (50 hosts):

$$\boldsymbol{Host\ válidos = 2^n - 2\ ;}$$

$$\boldsymbol{n = 6}$$

$$\boldsymbol{Host\ válidos = 62}$$

NY	Fastethernet 0/0	Máscara
Subred	172.31.127.0/26	255.255.255.192
Gateway	172.31.127.1/26	
Primera valida	172.31.127.2/26	
Ultima valida	172.31.127.62/26	
Broadcast	172.31.127.63/26	

Figura 24 Cálculo de subredes AS 100-NY.

Realizado por: *Morales, W. 2016.*

NY – Fa 0/1 (50 hosts):

$$\boldsymbol{Host\ válidos = 2^n - 2\ ;}$$

$$\boldsymbol{n = 6}$$

$$\boldsymbol{Host\ válidos = 62}$$

NY	Fastethernet 0/1	Máscara
Subred	172.31.127.64/26	255.255.255.192
Gateway	172.31.127.65/26	
Primera valida	172.31.127.66/26	
Ultima valida	172.31.127.126/26	
Broadcast	172.31.127.127/26	

Figura 25 Cálculo de subredes AS 100-NY.

Realizado por: *Morales, W. 2016.*

5.2. Protocolos de enrutamiento

El presente trabajo de titulación tiene como objetivo demostrar la capacidad de convergencia de múltiples tablas de enrutamiento usando diversos protocolos dinámicos, ya sean propietarios como EIGRP (Cisco), como estándares abiertos como IS-IS.

Dentro del AS público 100 convergen protocolos de enrutamiento como:

- *EIGRP*
- *OSPF*
- *Frame-Relay*
- *RIPv2*
- *BGP*

Se usan estos protocolos de enrutamiento por sus diversos beneficios tanto en la posibilidad de uso de VLSM, actualizaciones periódicas, poco consumo de ciclos de CPU, así como redistribución de rutas entre ellos, así como también se ha tenido en consideración ciertas debilidades en cada uno de ellos como adaptabilidad, velocidad de convergencia, escalabilidad en algunos casos Tomando en consideración que un protocolo de enrutamiento cumple un rol importante al momento de unir redes de tipo escalable como la presente, un protocolo de enrutamiento es el encargado y responsable de establecer reglas y políticas de cómo los routers se comunican con el resto de equipos, además de escoger el mejor camino entre múltiples que pudieran haber para enviar paquetes y actualizaciones al resto de la topología.

Los protocolos de enrutamiento pueden dividirse en dos grupos:

- *Interior Gateway Protocols:*
  - *Protocolos Vector Distancia (RIP, IGRP, EIGRP)*
  - *Protocolos de Estado de Enlace (IS-IS, OSPF)*
- *Exterior Gateway Protocols:*
  - *BGP*

ENRUTAMIENTO ESTÁTICO vs ENRUTAMIENTO DINÁMICO.-

El enrutamiento estático es un proceso mediante el cuál la tabla de enrutamiento se alimenta de forma manual por parte del administrador, por cada cambio que se diera en la topología como el aumentar el número de routers en la red es necesario la actualización de la tabla de rutas. Se usa con frecuencia en redes de tamaño pequeño que no tenga grandes planes de escalabilidad.

El enrutamiento estático brinda mayor seguridad que protocolos de enrutamiento dinámico, además de consumir pocos ciclos de CPU del equipo.

La desventaja de este tipo de enrutamiento es el pobre desempeño de la red cuando hay cambios topológicos o planes de escalar la red.

SUMARIZACIÓN.-

La sumarización es la técnica ampliamente utilizada que permite al protocolo de enrutamiento minimizar su tabla de enrutamiento cuando publique una ruta menor a la red o subred de destino. Las tablas de enrutamiento enviadas en cada actualización consumen valioso ancho de banda, por lo que sobre una red costosa como un enlace WAN tiene mucho sentido aplicar sumarización para comprimir las tablas de enrutamiento, además que depende la cantidad de rutas específicas que contenga la tabla de enrutamiento y el consumo de ciclos de CPU en los routers; esto afecta colateralmente al delay de la red, por lo que se podrá incrementar.

La sumarización es una herramienta que permite comprimir las tablas de rutas para hacerlas de tipo jerárquico, algunos beneficios de la sumarización:

- *Reducción del tamaño de tablas de enrutamiento*
- *Mayor velocidad de convergencia*
- *Escalabilidad*
- *Uso de recursos del router*
- *Mantenimiento*

Es importante recalcar que, si la topología de red tuviese un rango de direcciones discontinuas tal como por ejemplo 131.110.1.0/24 y 131.110.10.0/2, la técnica de sumarización no sería posible realizarla. Existen muchos protocolos de enrutamiento que aceptan procesos de sumarización de forma automática tal como RIPv2 o EIGRP, cuando sucede esto las redes anunciadas serán de tipo Classfull, es decir redes de clase Clase A con una máscara /8, redes de clase B con una máscara /16, redes de clase C con una máscara /24. En estos casos se puede desactivar la sumarización y hacerla de forma manual con el objetivo de permitir el anuncio o la publicación de ciertas rutas más específicas. También es importante recalcar que la sumarización manual puede ser aplicada en las interfaces del router.

Existen protocolos de enrutamiento tal como OSPF, donde se puede aplicar sumarizaciones manuales en las interfaces que se encuentran en el borde del área, tal es el caso de los routers de frontera (ABR), el cual puede manejar 2 ó más áreas.

5.2.1.Protocolo de enrutamiento EIGRP

EIGRP es un protocolo basado en vector distancia, esto significa que para encontrar y formar nuevas adyacencias así como eliminarlas, despliega un algoritmo para recalcular las diferentes rutas hacia los destinos, éste es Diffusing Update Algorithm (DUAL). EIGRP es un algoritmo basado en "Rumor" ya que el equipo posee una visión parcial de la topología confiando en la información que sus vecinos pueden proveer, con estos datos, el router añade la métrica que le cuesta llegar al vecino más cercano y así obtener un coste total del path comprendido entre el origen y destino, esto es: Distancia Factible.

Características:

- *Facilidad de trabajo en IPV4 e IPV6, además de ser compatible con otros protocolos de capa 3 como IPX y Apple Talk gracias a módulos PDM los cuales hacen posible manejar 3 tipos de tablas:*
    - *Tabla de vecindad*
    - *Tabla topológica*

- *Tabla de enrutamiento*

- *EIGRP usa RTP (Reliable Transport Procolo) para entregas confiables. Significa que al salir un paquete por ejemplo, un Update; el vecino ve la necesidad de confirmar la llegada de dicho paquete a través de un Acuse de recibo o Acknowledgement (ACK).*
- *EIGRP usa RTP (Real Time Protocol). Al salir el paquete de un router, es necesario introducir un número de secuencia a dicho paquete de modo que, al arrivar al receptor se notifique un ACK de ese número de secuencia.*
- *EIGRP utiliza DUAL (Diffusing Update Algorithm) para lo siguiente:*
    - *Encontrar una ruta de respaldo o backup en caso de caerse la ruta con la mejor (menor) métrica, es entonces cuando DUAL buscará una ruta con la segunda mejor métrica en la tabla topológica y la pricipalizará poniéndola en la tabla de rutas.*
    - *DUAL también es el encargado de verificar y garantizar que todas las rutas que están en la tabla de enrutamiento se encuentren libres de bucles o loops, para esto usa Split Horizon (Horizonte Dividido) con el fin de NO anunciar o publicar rutas por una interface por donde ya aprendió dicha ruta.*

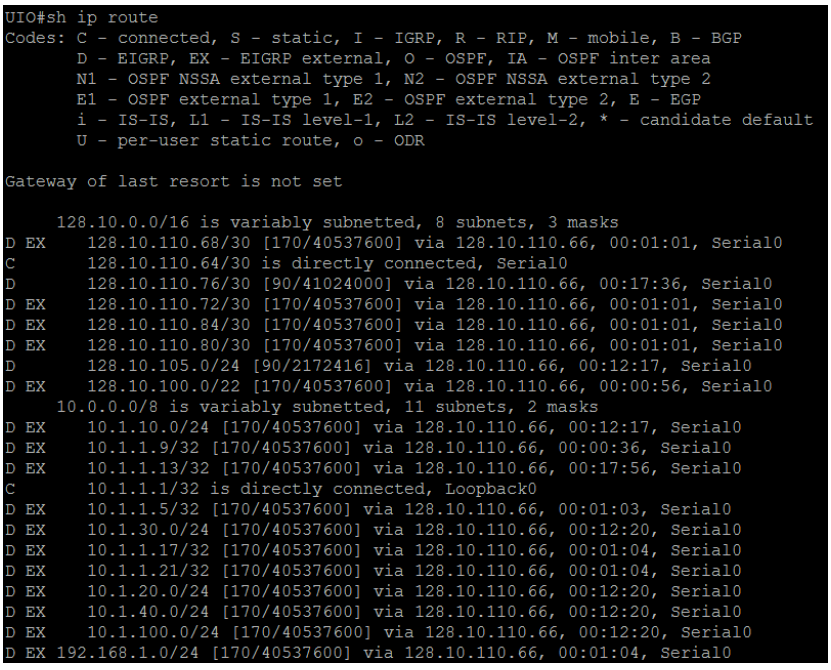


Figura 26 Tabla de enrutamiento-UIO

Realizado por: *Morales, W. 2016.*

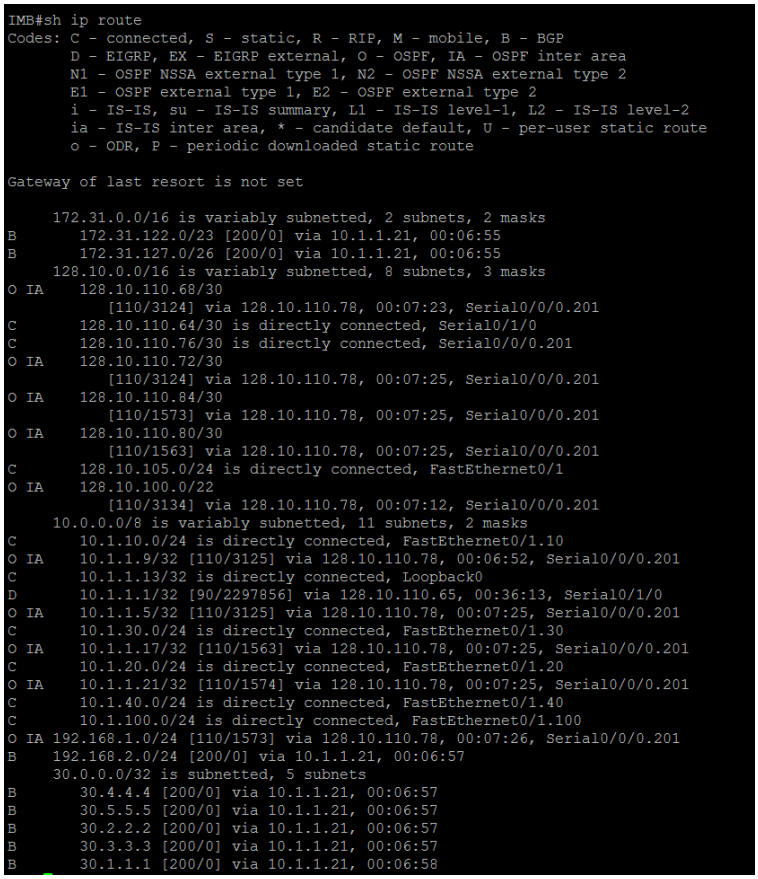


Figura 27 Tabla de enrutamiento-IMB

Realizado por: *Morales, W. 2016.*

EIGRP maneja 3 tipos de tablas de información según la tecnología que se utilice:

- *Tabla de vecindad.- Tabla donde se listan todos los neighbors que se encuentran en la topología.*
- *Tabla de rutas.- La cual contiene todos los mejores caminos o paths que ha podido calcular el algoritmo matemático DUAL hacia todos los destinos.*
- *Tabla topológica.- Tabla donde se muestran todos los posibles caminos y sus métricas que se podrían tener en caso que las rutas con los costes más bajos hayan desaparecido de la tabla de rutas.*

En la tabla de enrutamiento de UIO se puede observar la ruta sumarizada 128.10.0.0/16, la cual contiene 8 subredes de todas las interfaces seriales hacia los demás routers del AS100 conocidas por DUAL. Se destaca que cinco de las rutas, tienen AD (Distancia Administrativa) de un prefijo de un protocolo externo redistribuido [170].

En la ruta sumarizada 10.0.0.8/8, se destaca que once de las rutas, tienen una AD de un prefijo cuyo protocolo externo es redistribuido [170].

Para el caso del router IMB, se tiene la ruta hacia la dirección de loopback hacia UIO con una distancia administrativa de 90, lo cual significa que proviene de un prefijo interno. Es conocido por la interfaz S1 de IMB, con una Distancia Factible de 2297856.

Se puede observar de igual forma que se han podido levantar todas las sesiones iBGP usando las direcciones loopback de los routers de los Sistemas Autónomos AS100-AS400 con una Distancia Administrativa de 200 representando sesiones internas de BGP con su respectivo next-hop. Se ha procedido a sumarizar las rutas hacia el Route-Reflector (CCA), con el objetivo de no hacer tan pesada la tabla de enrutamiento y en cierta forma aplicar QoS, si por algún motivo flapea la sesión iBGP entre cualquiera de los routers internos de AS100, GYE siempre tendrá la ruta sumarizada apuntando a null. Con esto se asegura que no existan olas de enrutamiento en el Internet.

Esto resulta ser beneficioso ya que podemos evitar penalizaciones por dampening como forma de prevenir alteraciones en las rutas que se podría estar aprendiendo de R2-ISP1.

Se puede observar por parte de OSPF que todas las rutas de este protocolo son IA (Inter-Área), lo cual significa que están circulando LSAs de tipo 3 que han sido inyectadas por el ABR que en la presente topología es CCA. Este router posee 2 diferentes base de datos Link-State (una por cada área) y consecuentemente toda la información de LSAs 1 y 2 que circulan de forma Intra-Área (dentro del área) deben ser sumarizados para que puedan cruzan sus respectivas áreas.

CCA tiene la obligación como un router ABR de publicar información sumarizada tal como la métrica de sus redes a otras áreas. Si un router interno como AMB quiere tener alcanzabilidad hacia GYE, deberá calcular la métrica que le cuesta llegar a CCA más la métrica que le inyecta en ABR, en este caso CCA.

Las rutas hacia el resto de interfaces tienen una distancia administrativa de 90, lo cual indica que proviene de un prefijo interno cuyo enlace es Punto-Multipunto, el cual interconecta a los spokes a través del router hub.

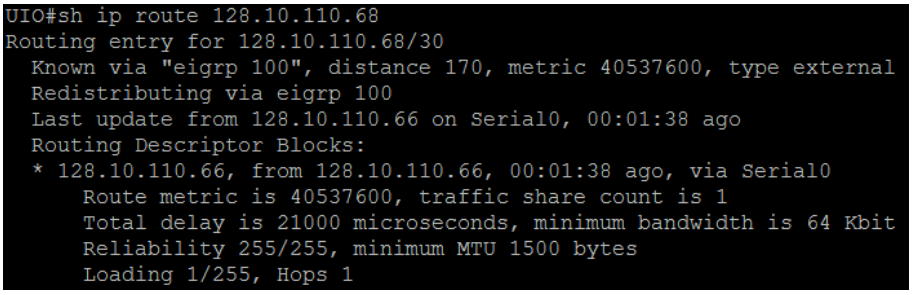


Figura 28 Ruta específica-UIO

Realizado por: *Morales, W. 2016.*

La distancia factible de UIO hacia las subredes que interconectan con los demás routers del AS es 40537600, conectándose por la interfaz 128.10.110.66 que representa la interface Serial S1 del router IMB para tener alcanzabilidad hacia el resto de equipos. La relación de vecindad con este router se realizó aproximadamente hace 1 minuto a través de la interface Serial 0 de UIO.

También se puede observar que se cumple con los tiempos que maneja por defecto de EIGRP para formar adyacencias, esto es en el caso de interfaces de capacidades bajas como seriales o enlaces WAN con un periodo de envío de paquetes Hello cada 60 segundos.

Cuando se practica la sumarización de todas las rutas en una sola, los vecinos EIGRP verán tan solo una ruta global, mas no las rutas específicas. Se puede plantear un escenario donde si los vecinos desearan ver las rutas específicas en cada actualización incremental se debería crear una ACL (Lista de Control de Acceso), la cual permita publicar las rutas más específicas que se necesite anunciar al vecino con su respectiva wildcard. Para luego crear un route-map que permita hacer match con la ACL en cuestión. Esta opción podría ser una forma de "Manipular el tráfico" dentro del IGP sin utilizar BGP. Se aplica la técnica de sumarización con el objetivo de:

- *Reducir el procesamiento del CPU del router.*
- *Reducir el tamaño de la tabla de rutas.*
- *Disminuir los tiempos de convergencia de las tablas de información.*
- *Facilitar los cálculos del algoritmo DUAL.*
- *Reducción de actualizaciones incrementales.- Si alguna de las rutas más específicas llegase a caer, el neighbor con el cual se estableció la relación de vecindad lo seguiría mirando de forma transparente; ya que inclusive al caer la ruta específica seguirá siendo alcanzable la ruta global sumarizada que deberá apuntar hacia NULL.*

```
UIO#sh ip inter brie
Interface              IP-Address      OK? Method Status                Protocol
Ethernet0              128.10.108.1    YES NVRAM  up                    down
Loopback0              10.1.1.1        YES NVRAM  up                    up
Serial0                128.10.110.65   YES NVRAM  up                    up
Serial1                unassigned      YES unset  administratively down down
IMB#sh ip inter brie
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            128.10.104.1    YES NVRAM  up                    down
FastEthernet0/1            128.10.105.1    YES NVRAM  up                    up
FastEthernet0/1.10         10.1.10.2       YES NVRAM  up                    up
FastEthernet0/1.20         10.1.20.2       YES NVRAM  up                    up
FastEthernet0/1.30         10.1.30.2       YES NVRAM  up                    up
FastEthernet0/1.40         10.1.40.2       YES NVRAM  up                    up
FastEthernet0/1.100        10.1.100.2      YES NVRAM  up                    up
Serial0/0/0                unassigned      YES NVRAM  up                    up
Serial0/0/0.201            128.10.110.77   YES NVRAM  up                    up
Serial0/1/0                128.10.110.66   YES NVRAM  up                    up
Serial0/2/0                unassigned      YES NVRAM  administratively down down
Serial0/3/0                unassigned      YES NVRAM  administratively down down
Loopback0                  10.1.1.13       YES NVRAM  up                    up
```

Figura 29 Tabla de enrutamiento-UIO

Realizado por: *Morales, W. 2016.*

Las interfaces de UIO están configuradas de acuerdo al plan de direccionamiento VLSM, se optó por configurar interfaces loopback en los routers que manejan el IGP, con el fin de levantar sesiones iBGP entre los peerings que llevarán prefijos e información de enrutamiento de los clientes. Se puede optar por manejar el next-hop para levantar la adyacencia de BGP usando cualquier otro tipo de interfaz física, pero la ventaja es que las direcciones de loopback son virtuales, razón por la cual implica que nunca caerá mientras no se aplique el comando shutdown en la misma. La interfaz de loopback no caerá inclusive si la interfaz física hace Flapping mientras tenga enlaces redundantes con algún vecino.

La dirección de Loopback 10.1.1.1 (UIO), tiene máscara /32 con el objetivo que no sea dependiente del IGP y no ser parte del enrutamiento interno del AS100.

```
UIO#sh ip eigrp topology
IP-EIGRP Topology Table for process 100

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 10.1.1.9/32, 1 successors, FD is 40537600
         via 128.10.110.66 (40537600/40025600), Serial0
P 10.1.1.13/32, 1 successors, FD is 40537600
         via 128.10.110.66 (40537600/40025600), Serial0
P 10.1.1.1/32, 1 successors, FD is 128256
         via Connected, Loopback0
P 10.1.1.5/32, 1 successors, FD is 40537600
         via 128.10.110.66 (40537600/40025600), Serial0
P 10.1.1.17/32, 1 successors, FD is 40537600
         via 128.10.110.66 (40537600/40025600), Serial0
P 10.1.1.21/32, 1 successors, FD is 40537600
         via 128.10.110.66 (40537600/40025600), Serial0
P 192.168.1.0/24, 1 successors, FD is 40537600
         via 128.10.110.66 (40537600/40025600), Serial0
P 128.10.110.68/30, 1 successors, FD is 40537600
         via 128.10.110.66 (40537600/40025600), Serial0
P 128.10.110.64/30, 1 successors, FD is 2169856
         via Connected, Serial0

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 128.10.110.76/30, 1 successors, FD is 41024000
         via 128.10.110.66 (41024000/40512000), Serial0
P 128.10.110.72/30, 1 successors, FD is 40537600
         via 128.10.110.66 (40537600/40025600), Serial0
P 128.10.110.84/30, 1 successors, FD is 40537600
         via 128.10.110.66 (40537600/40025600), Serial0
P 128.10.110.80/30, 1 successors, FD is 40537600
         via 128.10.110.66 (40537600/40025600), Serial0
```

Figura 30 Tabla topológica-UIO

Realizado por: *Morales, W. 2016.*

```
IMB#sh ip eigrp topology
IP-EIGRP Topology Table for AS(100)/ID(10.1.1.13)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 10.1.1.9/32, 1 successors, FD is 40025600
        via Redistributed (40025600/0)
P 10.1.1.13/32, 1 successors, FD is 40025600
        via Redistributed (40025600/0)
P 10.1.1.1/32, 1 successors, FD is 2297856
        via 128.10.110.65 (2297856/128256), Serial0/1/0
P 10.1.1.5/32, 1 successors, FD is 40025600
        via Redistributed (40025600/0)
P 10.1.1.17/32, 1 successors, FD is 40025600
        via Redistributed (40025600/0)
P 10.1.1.21/32, 1 successors, FD is 40025600
        via Redistributed (40025600/0)
P 192.168.1.0/24, 1 successors, FD is 40025600
        via Redistributed (40025600/0)
P 128.10.110.68/30, 1 successors, FD is 40025600
        via Redistributed (40025600/0)
P 128.10.110.64/30, 1 successors, FD is 2169856
        via Connected, Serial0/1/0

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 128.10.110.76/30, 1 successors, FD is 40512000
        via Connected, Serial0/0/0.201
P 128.10.110.72/30, 1 successors, FD is 40025600
        via Redistributed (40025600/0)
P 128.10.110.84/30, 1 successors, FD is 40025600
        via Redistributed (40025600/0)
P 128.10.110.80/30, 1 successors, FD is 40025600
        via Redistributed (40025600/0)
```

Figura 31 Tabla topológica-IMB

Realizado por: *Morales, W. 2016.*

```
R3_ISP1#sh ip eigrp topology
IP-EIGRP Topology Table for AS(200)/ID(20.3.3.3)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 20.1.1.1/32, 1 successors, FD is 25122560
        via 150.1.2.1 (25122560/25120000), FastEthernet0/1
P 20.2.2.2/32, 1 successors, FD is 25122560
        via 150.1.3.1 (25122560/25120000), FastEthernet0/0
P 20.3.3.3/32, 1 successors, FD is 25120000
        via Redistributed (25120000/0)
P 150.1.3.0/24, 1 successors, FD is 2816
        via Connected, FastEthernet0/0
P 150.1.2.0/24, 1 successors, FD is 2816
        via Connected, FastEthernet0/1
P 150.1.1.0/24, 2 successors, FD is 5376
        via 150.1.2.1 (5376/2816), FastEthernet0/1
        via 150.1.3.1 (5376/2816), FastEthernet0/0
R2_ISP1#sh ip eigrp topology
IP-EIGRP Topology Table for AS(200)/ID(20.2.2.2)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 20.1.1.1/32, 1 successors, FD is 25122560
        via 150.1.1.1 (25122560/25120000), GigabitEthernet0/0
P 20.2.2.2/32, 1 successors, FD is 25120000
        via Redistributed (25120000/0)
P 20.3.3.3/32, 1 successors, FD is 25122560
        via 150.1.3.2 (25122560/25120000), GigabitEthernet0/1
P 150.1.3.0/24, 1 successors, FD is 2816
        via Connected, GigabitEthernet0/1
P 150.1.2.0/24, 2 successors, FD is 5376
        via 150.1.1.1 (5376/2816), GigabitEthernet0/0
        via 150.1.3.2 (5376/2816), GigabitEthernet0/1
P 150.1.1.0/24, 1 successors, FD is 2816
        via Connected, GigabitEthernet0/0
R1_ISP1#sh ip eigrp topology
IP-EIGRP Topology Table for AS(200)/ID(20.1.1.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 20.1.1.1/32, 1 successors, FD is 25120000
        via Redistributed (25120000/0)
P 20.2.2.2/32, 1 successors, FD is 25122560
        via 150.1.1.2 (25122560/25120000), FastEthernet0/1
P 20.3.3.3/32, 1 successors, FD is 25122560
        via 150.1.2.2 (25122560/25120000), FastEthernet0/0
P 150.1.3.0/24, 2 successors, FD is 5376
        via 150.1.1.2 (5376/2816), FastEthernet0/1
        via 150.1.2.2 (5376/2816), FastEthernet0/0
P 150.1.2.0/24, 1 successors, FD is 2816
        via Connected, FastEthernet0/0
P 150.1.1.0/24, 1 successors, FD is 2816
        via Connected, FastEthernet0/1
```

Figura 32 Tablas topológicas-R1, R2, R3_ISP1

Realizado por: *Morales, W. 2016.*

Paquetes QUERY y REPLAY (Escenario).-

Suponiendo que las redes GYE-WA estarían dentro un Sistema Autónomo, y habiéndose escogido como el mejor camino (menor métrica) el enlace GYE, R2_ISP1, R1_ISP1, R3_ISP1, WA. Siendo R1 el successor y al caer éste router, se tiene:

Si DUAL hubiera escogido al successor factible cuando se dio por muerto R1_ISP1, R3_ISP1 automáticamente hubiera pricipalizado la ruta GYE, R2_ISP1, R3_ISP1, WA y se hubiera catalogado como sucesor a R3_ISP1 y la red podría funcionar normalmente sin problemas.

Al no ser así, DUAL buscará en la tabla topológica de GYE al successor factible, si no lo tiene el router entra a un estado "Activo" dando inicio a un contador de 3 min para que se pueda encontrar la solución. Para esto GYE envía mediante multicast paquetes Query a todos sus vecinos intentando averiguar si alguno de ellos conoce cómo llegar al destino, teniendo dos posibilidades: que nadie sepa cómo llegar al destino o que alguien finalmente sepa la forma de llegar al destino. Cada respuesta que se emite como contestación de un paquete Query se llama Replay.

Cada paquete Query se envía mediante direccionamiento multicast, esperando confirmaciones mediante Unicast.

EIGRP maneja los siguientes paquetes:

Paquetes UPDATE.- *Son actualizaciones enviadas hacia routers vecinos. Usa RTP (Reliable Transport Protocol) como mecanismo de autenticación de vecindad, para esto el router transmisor del paquete crea un usuario y una pregunta (llaves), la misma que debe ser contestada correctamente por el receptor con el fin de poder leer el paquete.*

EIGRP tiene 2 formas actualizaciones:

- *Actualizaciones Incrementales.- La ventaja de EIGRP frente a otros protocolos de enrutamiento como RIP es que no se envía de manera periódica toda la tabla de enrutamiento, sino únicamente cuando hay un cambio topológico se envía dicha actualización con el cambio ocurrido en ese instante.*

- *Actualizaciones Totales.- La única vez que un router envía toda la tabla de enrutamiento es cuando descubre a un nuevo vecino y forma una adyacencia.*

Todas las posibles redes alcanzadas así como sus respectivos costes se encuentran en estado "Passive", esto es bueno ya que la topología no ha entrado en conflicto. Es posible alcanzar a todas las rutas por las Interfaz Serial 0 del router UIO.

Es por este motivo que EIGRP es un protocolo basado en "Rumor", ya que el router UIO confía en la métrica (Distancia Notificada) anunciada por IMB para alcanzar al resto de neighbors. UIO añade su coste para llegar a IMB, y así obtiene una métrica total (Distancia Factible)

Según los datos proporcionados, se tiene:

$$\boldsymbol{Distancia\ Factible} = Coste\ hacia\ el\ vecino\ más\ cercano + Distancia\ Notificada$$

- *Métrica entre UIO y Neigbors: [512000]*
- *Distancia Notificada: [40025600]*
- *Distancia Factible: [405376000]*

Para interfaz WAN del Área 100 (NSSA) se tiene:

- *Métrica entre UIO y FR1: [512000]*
- *Distancia Notificada: [40512000]*
- *Distancia Factible: [41024000]*
- *Distancia Factible para dirección Loopback de UIO: [128256]*
- *Distancia Factible para interfaz serial de IMB: [2169856]*

Cuando se realiza el proceso de adyacencia EIGRP, DUAL realiza cálculos matemáticos para identificar los mejores caminos hacia las diferentes rutas existentes. Cuando la red converge, DUAL pone en la tabla de rutas los paths que tienen los mejores costos, quedando en la tabla topológica las demás rutas con la segunda mejor métrica.

Cuando una ruta presente en la tabla de enrutamiento deja de existir, la topología entra a un proceso de Query o Active el cual hace que se active un timer de 3 minutos para que inmediatamente DUAL realice la búsqueda dentro de la tabla topológica de una ruta de backup previamente escogida. En el caso de no haber ningún sucesor factible en la tabla topológica, el router que sufrió el cambio enviará paquetes llamados Queries de forma intermitente en modo multicast usando la dirección 224.0.0.10 hasta 16 veces o hasta cuando un vecino responda un replay para dar a conocer que dicho neighbor tiene una entrada que coincide con la red perdida. A la segunda vez que se envíe Quieries el router lo hará en unicast.

Si ningún vecino conoce como llegar al destino, la topología entra a un estado llamado SIA (Stuck in Active), finaliza el proceso Query y la ruta se da finalmente como perdida.

- *EIGRP utiliza paquetes Hello para encontrar y formar nuevas adyacencias con otros routers, así como para detectar que una sesión EIGRP ha caído.*

```
UIO#sh ip eigrp neighbors
IP-EIGRP neighbors for process 100
H   Address                 Interface   Hold Uptime   SRTT   RTO  Q  Seq
                                        (sec)         (ms)       Cnt Num
0   128.10.110.66           Se0           10 00:15:46   28   200  0  20
IMB#sh ip eigrp neighbors
IP-EIGRP neighbors for process 100
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
0   128.10.110.65           Se0/1/0           11 00:20:17   31   200  0  17
R3_ISP1#sh ip eigrp neighbors
IP-EIGRP neighbors for process 200
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
1   150.1.3.1               Fa0/0             13 01:48:18  626  3756  0  14
0   150.1.2.1               Fa0/1             13 01:48:18  654  3924  0  14
R2_ISP1#sh ip eigrp neighbors
IP-EIGRP neighbors for process 200
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
1   150.1.3.2               Gi0/1             13 01:57:09   12   200  0  11
0   150.1.1.1               Gi0/0             11 02:01:27  521  3126  0  11
R1_ISP1#sh ip eigrp neighbors
IP-EIGRP neighbors for process 200
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
1   150.1.2.2               Fa0/0             14 02:01:48    6   200  0  12
0   150.1.1.2               Fa0/1             13 02:06:06    1   200  0  11
```

Figura 33 Tabla de vecindades-UIO, IMB, R1, R2, R3_ISP1.

Realizado por: *Morales, W. 2016.*

EIGRP es un protocolo parcialmente propietario de Cisco, debido a que si bien es cierto se liberó el protocolo para ser interoperable entre otros estándares, Cisco no ha liberado algunos algoritmos matemáticos (Timers) por completo, los cuales son las bases del motor de búsqueda que usa DUAL para encontrar los mejores paths hacia un destino, estos son:

- *SRTT (Smooth Round Time Trip): Es un timer o temporizador medido en [ms], el cual se activa al momento de enviar por ejemplo un update, es el tiempo medido desde que sale el paquete del router hasta recibir un ACK como notificación de respuesta del vecino.*

  Del SRTT se desprenden los siguientes timers:
- *MTF (Multicast Time Flow): Temporizador que empieza a correr junto al SRTT, cuando este contador expira sin que haya un ACK como repuesta del vecino, la siguiente re transmisión del paquete a enviarse ya no será en multicast (224.0.0.10) sino en Unicast, automáticamente se activa el temporizador RTO.*
- *RTO (Re- transmission Time Out): Es el tiempo que existe entre re transmisiones (máximo hasta 16 re transmisiones en Unicast)*

EIGRP maneja para su funcionamiento el uso de paquetes, tales como:

- *Paquetes HELLO.- Son paquetes enviados periódicamente a través de la red de forma constante cada 5 segundos en un ambiente de LAN (redes punto-punto o multipunto) donde hay velocidades altas mayores a 1 T1 (1544 Kbps), y cada 60 segundos en un ambiente WAN donde hay velocidades bajas y menores a 1 T1, además de ser enviados usando la dirección multicast 224.0.0.10.*

  Una variante de los paquetes Hello es el llamado Hold Time, el cual por defecto es 3 veces el tiempo de Hello, lo que significa que si en 15 segundos no hay respuesta de un vecino en un ambiente LAN, éste será dado por caído. Lo mismo para enlaces WAN (180 segundos).

Dentro de cada paquete Hello se envía la siguiente información:

- *IP*
- *Sistema Autónomo (AS)*
- *Valores de K (Para el cálculo de la métrica)*
- *Hold Time (Esto sirve a un router para conocer cuánto tiempo máximo puede esperar sin tener noticias del origen)*

Hay que destacar que para que dos routers levanten sesiones EIGRP deben necesariamente:

- *Compartir paquetes Hello*
- *Ser parte del mismo AS*
- *Compartir los mismos valores K para el cálculo de la métrica.*

EIGRP maneja dos tipos de actualizaciones:

- *Actualizaciones Incrementales.- EIGRP al ser un protocolo basado en DUAL tiene como finalidad no consumir demasiados recursos como el ancho de banda, por lo que no actúa como protocolos de enrutamiento como RIP; enviando toda la tabla de enrutamiento en forma de actualizaciones cada 30 segundos. Sino más bien por el contrario, sólo cuando existe un cambio topológico en la red se envía la porción de red que cambió en ese instante.*
- *Actualizaciones Multicast.- EIGRP utiliza RTP (Reliable Transfer Protocol) para enviar sus actualizaciones usando direccionamiento multicast (224.0.0.10) y cuando recibe un ACK como notificación de recepción del paquete Update lo hace en Unicast. Es un aspecto mejorado de otros protocolos de enrutamiento que manejan actualizaciones basadas en direccionamiento tipo broadcast.*

EIGRP es un protocolo de enrutamiento Classless, lo cual significa que se envían tanto la máscara y el prefijo de subred en cada paquete enviado hacia los vecinos, además soporta

VLSM, CIDR, y sumarización; e indirectamente al hablar de sumarización se entiende que EIGRP sirve para la construcción de redes escalables (grandes).

DUAL tiene la compleja tarea de encontrar y escoger los mejores caminos sin bucles hacia los destinos usando como parámetros el ancho de banda y el retardo, además de almacenar rutas de respaldo (Sucesor Factible) para destinos que tengan más de un path de comunicación ya que puede soportar hasta un máximo de 4 vías con balanceo de carga o Load Sharing. El balanceo de carga que soporta EIGRP es de 4 rutas alternas hacia un destino con el mismo coste, es decir con la misma Distancia Factible; vale destacar que no todos los routers pueden participar de la elección para ser el router "Fisable Distance", para esto, el aspirante debe cumplir los siguientes requerimientos:

- *Distancia Notificada del router aspirante < Distancia Factible del router principal*
- *Distancia Factible del aspirante < Variance*Distancia Factible del router principal*

El parámetro Variance es una herramienta poderosa que ayuda a balancear el tráfico sobre paths con diferente costo, por lo que si existen cuatro rutas con el mismo coste hacia un destino, entran todos los paths en la tabla de enrutamiento.

EIGRP ofrece mayor capacidad de enrutamiento que su antecesor Interior Gateway Protocol (IGRP), ya que usa 32 bits para el cálculo de la métrica, y no 24 bits como lo hacía IGRP. Otra característica importante de EIGRP es que se auto-limita en el consumo de Ancho de Banda (Bandwidth) a no más del 50%, esto quiere decir que EIGRP no saturará nunca los enlaces por el envió de paquetes que contienen información de Routing. Este valor es configurable con el comando: ip bandwidth percent [valor]. De esta forma EIGRP cuida no saturar los enlaces lentos y con velocidades bajas como lo son los enlaces WAN.

Hay que tener en consideración que el AS en EIGRP solo tiene significado local, lo cual repercute que las publicaciones llegarán máximo al AS en cuestión.

EIGRP tiene tres clases de rutas con los siguientes costos:

- *Prefijo sumarizado (5)*
- *Prefijo interno (90)*
- *Prefijo de un protocolo externo y redistribuido (170)*

Se tomó en consideración EIGRP como parte de los protocolos de enrutamiento del AS100 ya que es usado muy frecuentemente cuando se trata de aplicaciones en tiempo real por su alto desempeño, cortos periodos de convergencia, jitter y delay en comparación de Open Shortest Path First (OSPF).

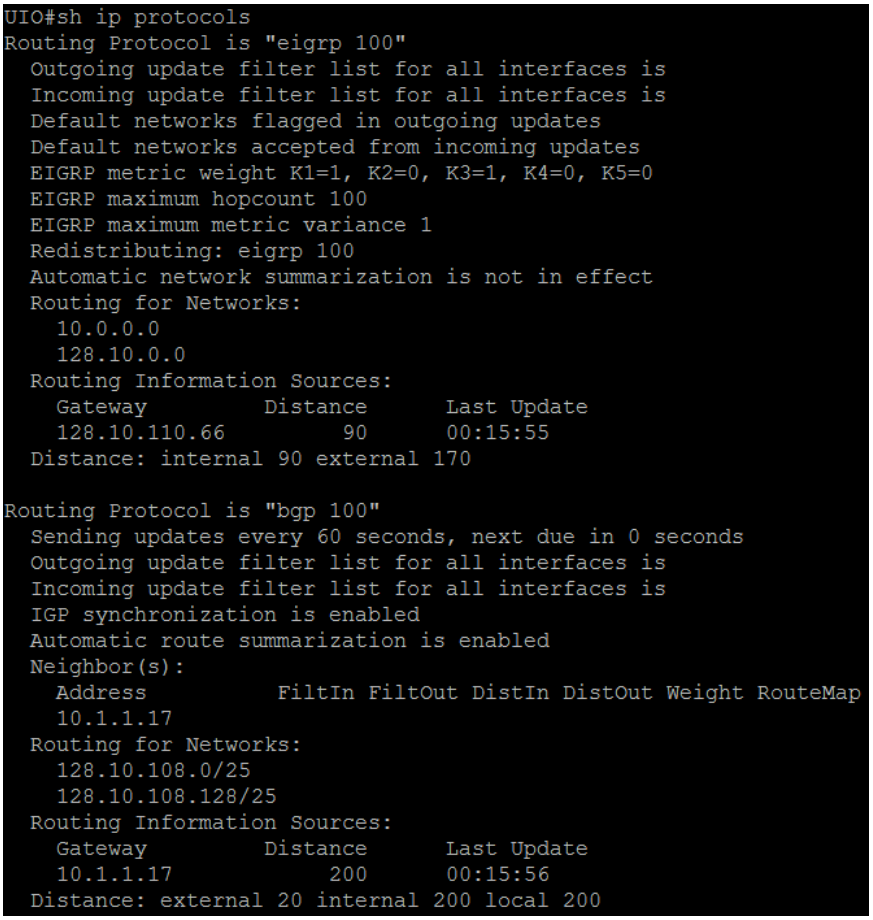
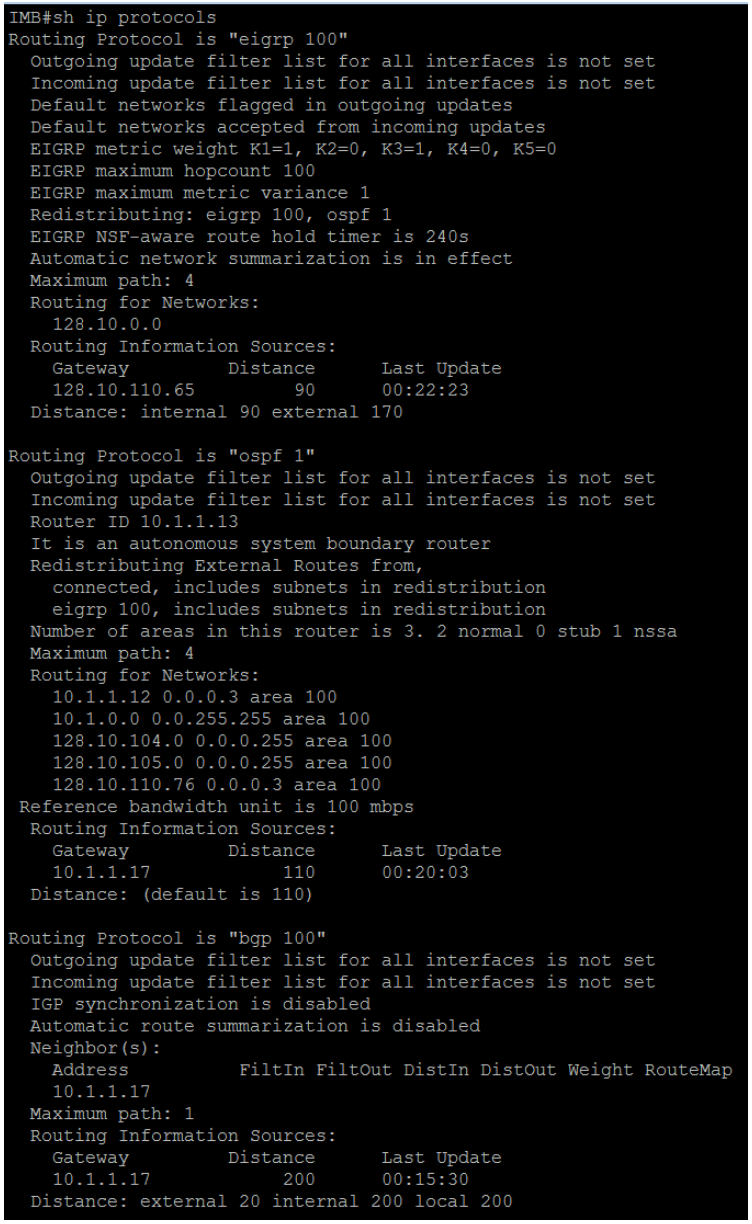


Figura 34 Información de protocolos-UIO.

Realizado por: *Morales, W. 2016.*



```
IMB#sh ip protocols
Routing Protocol is "eigrp 100"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 100, ospf 1
  EIGRP NSF-aware route hold timer is 240s
  Automatic network summarization is in effect
  Maximum path: 4
  Routing for Networks:
    128.10.0.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    128.10.110.65         90      00:22:23
  Distance: internal 90 external 170

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 10.1.1.13
  It is an autonomous system boundary router
  Redistributing External Routes from,
    connected, includes subnets in redistribution
    eigrp 100, includes subnets in redistribution
  Number of areas in this router is 3. 2 normal 0 stub 1 nssa
  Maximum path: 4
  Routing for Networks:
    10.1.1.12 0.0.0.3 area 100
    10.1.0.0 0.0.255.255 area 100
    128.10.104.0 0.0.0.255 area 100
    128.10.105.0 0.0.0.255 area 100
    128.10.110.76 0.0.0.3 area 100
 Reference bandwidth unit is 100 mbps
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.1.1.17            110      00:20:03
  Distance: (default is 110)

Routing Protocol is "bgp 100"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  IGP synchronization is disabled
  Automatic route summarization is disabled
  Neighbor(s):
    Address          FiltIn FiltOut DistIn DistOut Weight RouteMap
    10.1.1.17
  Maximum path: 1
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.1.1.17            200      00:15:30
  Distance: external 20 internal 200 local 200
```

Figura 35 Información de protocolos-IMB.

Realizado por: *Morales, W. 2016.*

Métrica

El valor de la métrica es utilizado con el fin de asignar un determinado coste para alcanzar un destino. La métrica determina la mejor ruta cuando existen múltiples vías para alcanzar un mismo destino. Cada protocolo de enrutamiento tiene su propio algoritmo para calcular el coste, por ejemplo Routing Information Protocol (RIP) se basa en la cantidad de saltos hacia un destino, el número máximo permitido es 16, OSPF basa su métrica en el ancho de banda de sus enlaces.

Cálculo de Métrica:

EIGRP maneja una métrica compuesta, ya que contiene algunos factores que afectan y determinan la forma de como calcular los mejores paths hacia los destinos.

Para calcular la métrica, EIGRP usa la siguiente formula:

$$Metrica = 256\left(K1 * AB + \frac{K2 * AB}{256 - Carga} + K3 * Delay\right) *$$

Ecuación 1 Cálculo de ancho de banda EIGRP

Donde:

- ***K1 (Ancho de banda).-*** *Se considera como el mínimo ancho de banda necesario que debe tener la interfaz, medido en [Kbps], viene dado en:* $\frac{10^7}{Enlace\ con < AB}$.

Medio	***Delay***
T1	*1544 Kbps*
DSO	*64 Kbps*

- ***K2 (Confiabilidad).-*** *Probabilidad existente para que un enlace falle, se mide dentro de confiabilidad en rangos de 1 a 255, siendo 1 el sinónimo de un enlace no confiable y 255 un enlace confiable.*
- ***K3 (Delay).-*** *Es el retardo y tiempo total que existe desde el inicio hasta el fin del path, medido en [ms]*

Medio	***Delay***
Fast Ethernet	*100 us*
Ethernet	*1000 us*
T1	*20000 us*

- ***K4 (Carga).-*** *Sinónimo de cuan saturado está el enlace, se mide en un rango de 1 a 255.*
- ***K5 (MTU).-*** *Maximum Transmission Unit, por defecto utiliza el mismo valor de Ethernet (1500 bytes).*

De todas estas constantes, Cisco utiliza por defecto: K1 y K3.

Seteando en la formula anterior K1=1, K2=0, K3=1, K4=0, K5=0, se tiene:

$$Metrica = 256(AB[Kbps] + Delay[us])$$

Finalmente:

$$Metrica = 256\left(\frac{10^7}{Enlace\ con\ < AB} + \frac{\Sigma\ Delays}{10}\right)$$

Ecuación 2 Ecuación final EIGRP

5.2.2.Protocolo de enrutamiento OSPF

Open Shortest Path First es un protocolo Classless que permite sumarización, VLSM, CIDR, lo cual permite que las redes sean de tipo escalables y de rápida convergencia gracias a su algoritmo matemático para calcular los mejores paths basado en el Ancho de Banda de los enlaces. Es un protocolo abierto e interoperable con distintos fabricantes que usa direccionamiento multicast para anunciar actualizaciones incrementales enviando LSAs al resto de la topología en redes back to back y Point to Multipoint.

CARACTERISTICAS.-

- *OSPF usa el enlace con el menor coste entre todos lo que hubiese para llegar al destino.*
- *Todos los routers dentro del área tienen la misma base de datos Link-State.*
- *OSPF está basado en áreas, esto con el objetivo de reducir ciclos de procesamiento en el CPU de routers.*
- *Cada área ejecuta su propio algoritmo matemático DIKSTRA.*

ÁREAS.-

- *El área 0 brinda conectividad entre áreas.*
- *Todo el tráfico generado entre áreas necesariamente debe pasar por el área de backbone y las actualizaciones intra-áreas se envían de forma sumarizada.*

- *Las áreas son creadas con el fin de agrupar routers que compartan la misma información o Base Datos, con esto se logra particionar la red en múltiples áreas expandiendo así la escalabilidad de la red.*
- *Cada vez que existe un cambio topológico en la red, el algoritmo Dijkstra re-calcula las rutas y envía actualizaciones dentro del área en cuestión.*

CLASIFICACION DE ROUTERS.-

OSPF define algunos tipos de routers según su función y posición dentro de la topología, estos son:

- ***Router interno.-*** *Este tipo de routers mantienen todas sus interfaces dentro de la misma área.*
- ***Router ABR (Area Border Router). -*** *Este tipo de routers mantiene 1 base de datos link-state por cada área adyacente, estos equipos conectan áreas y conocen las rutas a todos los destinos.*
- ***Router de backbone.-*** *Todas sus interfaces se encuentran dentro del área 0.*
- ***Router ASBR (Autonomous System Boundary Router). -*** *Estos routers se pueden comunicar con otros Sistemas Autónomos usando diversos protocolos de enrutamiento, pueden estar en cualquier lugar de la topología.*

ADYACENCIAS.-

Para que dos routers establezcan una adyacencia deben cumplir los siguientes requerimientos:

- *Las interfaces que unen los equipos deben pertenecer a la misma área.*
- *Las áreas que pertenecen los quipos deben ser del mismo tipo.*
- *El direccionamiento IP de las interfaces deben pertenecer a la misma subred.*
- *Ningún equipo debe tener configurado el mismo Router-ID*
- *Los timers deben coincidir (Hello time, Dead time).*
- *Los equipos deben manejar el mismo tipo de autenticación.*

Con estos requisitos cumplidos se puede garantizar que las sesiones OSPF no tendrán problemas con LSA's y todos los equipos llegarán sin problemas a pasar todas las fases de máquina de estados finitos y tener relaciones de vecindades sanas.

ESTABLECIMIENTO DE ADYACENCIAS.-

Para que dos equipos formen una relación de vecindad, deben cumplir 2 fases las cuales llevan a que los equipos tengan la misma base de datos del área:

- *Comunicación Bidireccional:*
  - ***Estado Down.-*** *No existe ninguna comunicación*
  - ***Estado Attempt.-*** *Esta fase existe únicamente cuando se configura manualmente un neighbors en redes Non Broadcast Multi-Access (NBMA), se envían paquetes Hello.*
  - ***Estado Init.-*** *El router recibe paquetes Hello del neighbor sin su Router-ID.*
  - ***Estado 2 Way.-*** *El router recibe paquetes Hello del neighbor con su Router-ID.*
- *Intercambio de información:*
  - ***Estado Exstart.-*** *Se desarrolla el proceso de elección del DR, e intercambo de LSAs.*
  - ***Estado Exchange.-*** *Intercambio de LSDBs, se usan ACKs como respuestas.*
  - ***Estado Louding.-*** *Los equipos hacen una espera para conocer si su neighbor tiene completa su base de datos Link-State, para esto usan LSRs, LSUs y LSACKs.*
  - ***Estado Full.-*** *Los equipos poseen la misma LSDB.*

Figura 36 Debugging-CCA.

Realizado por: *Morales, W. 2016.*

OSPF envía paquetes Hello al medio para detectar nuevos vecinos, es así como se alimentan las tablas de vecindad de este protocolo. Hay que tener en cuenta para que formen adyacencias los equipos es necesario que tengan los mismos timers.

- *Paquetes Hello son enviados en una LAN cada 10 segundos*
- *Paquetes Hello son enviados en una WAN cada 30 segundos*
- *El Dead Time es el tiempo máximo para que llegue un Hello del neighbor, por defecto es 4 veces el tiempo de Hello.*
- *El redes tipo Non Broadcast y Punto-multipunto el tiempo de Hello es 30 segundos y su Dead Time de 120 segundos.*
- *Para redes Broadcast y Punto-Punto, el tiempo de Hello es 10 segundos y su Dead Time de 0 segundos.*

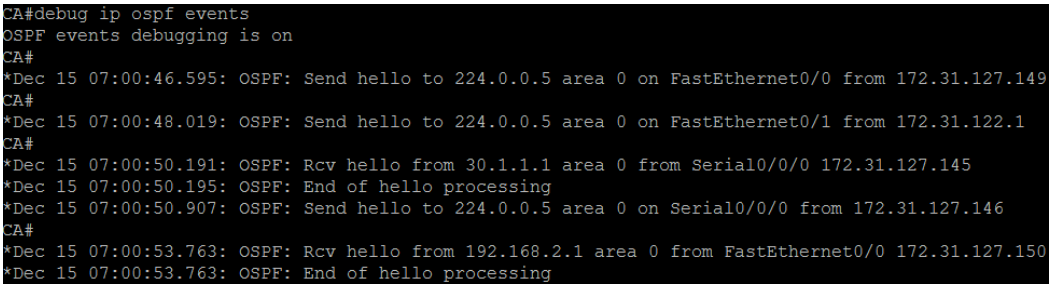


Figura 37 Debugging-CA.

Realizado por: *Morales, W. 2016.*

OSPF puede levantar sesiones con fallas cuando se configura diferentes tipos de red en cada extremo con los mismos timers, por ejemplo al configurar una interfaz como Broadcast y del otro lado como Punto-Punto pero tienen los mismos intervalos de Hello y Dead Time sí podrían levantar la sesión OSPF. El extremo configurado como Broadcast esperará la elección de un DR/BDR y del otro no, y aunque se levante la sesión OSPF los LSA's tendrán problemas y por ende la base de datos Link-State tendrá inconsistencias.

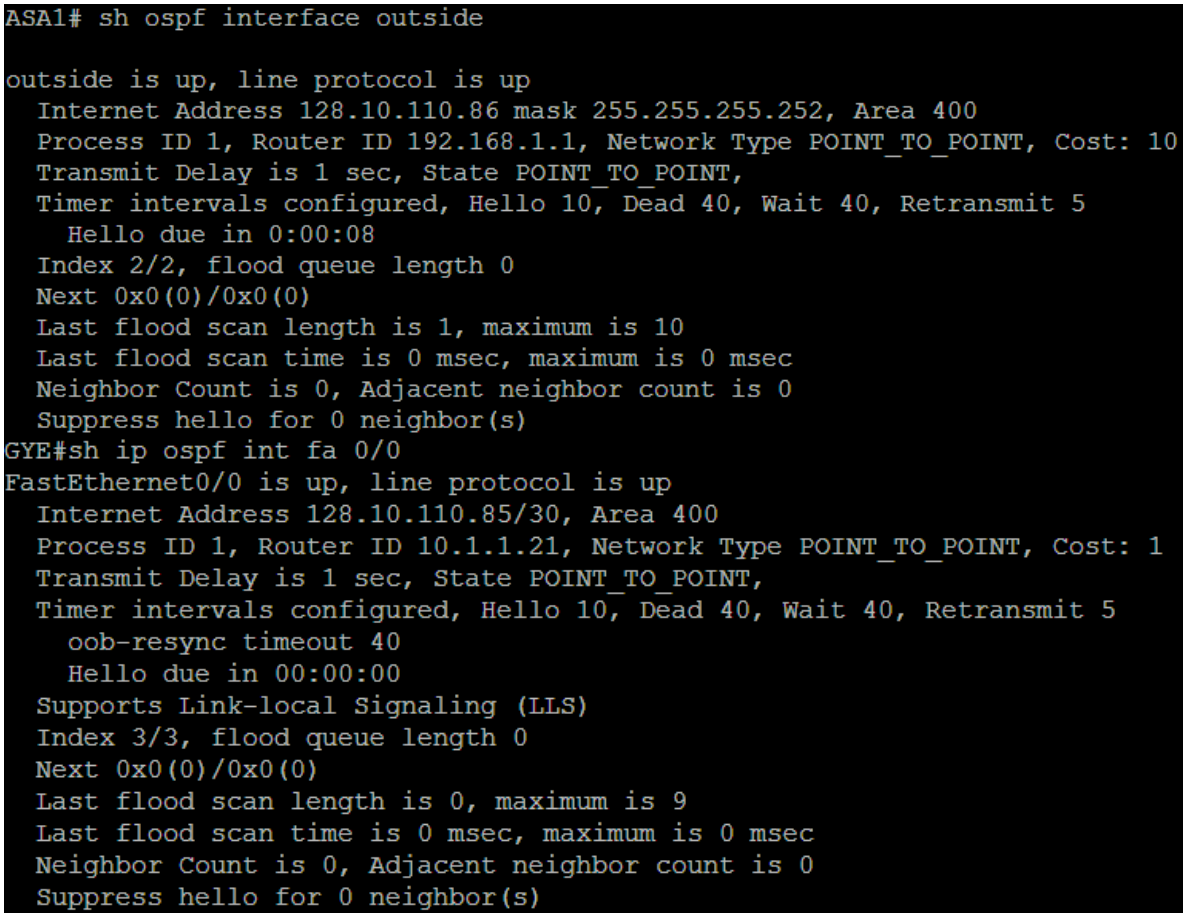
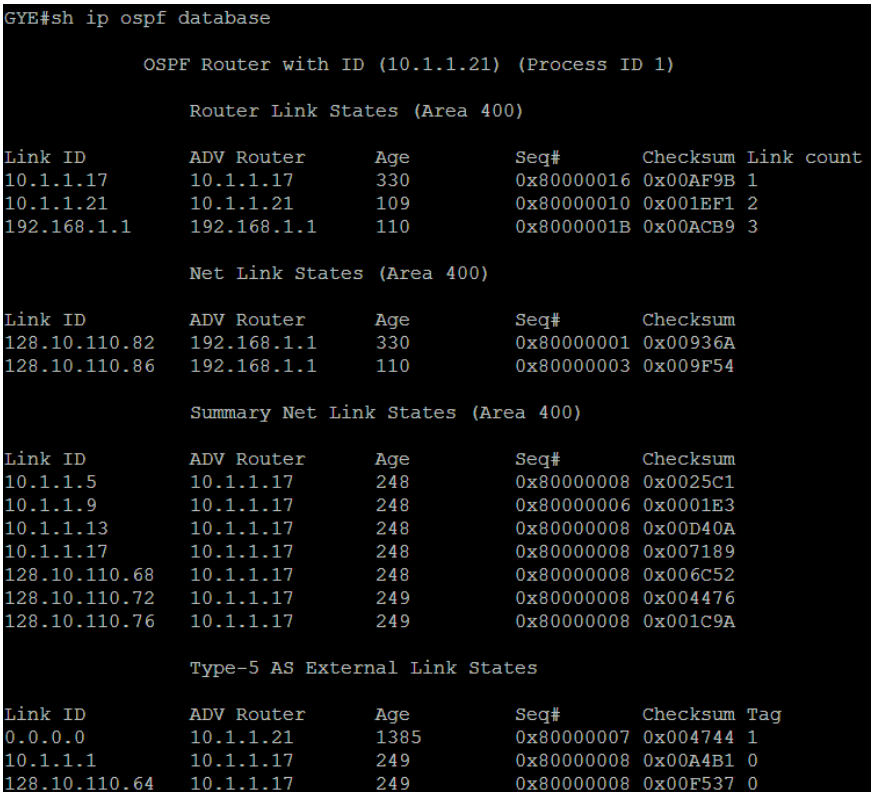


Figura 38 Interfaces OSPF-ASA1, GYE.

Realizado por: *Morales, W. 2016.*

El enlace que une el Firewall ASA1 con el router GYE es una interfaz Fastethernet, que por defecto es un medio multi-access donde se pueden establecer diversas adyacencias; sin embargo como solo unen 2 equipos y no se necesita formar más vecindades, lo correcto sería configurar las interfaces como Point-Point. Incluso si del lado del Firewall ASA se configura la interfaz outside como Broadcast, la adyacencia se formaría pero corriendo el riesgo que se generen LSAs de tipo 3 los cuales no serían compatibles con una red Punto-Punto, donde no existen estos mensajes puesto que carecen de un Router Designado (DR).



```
GYE#sh ip ospf database

            OSPF Router with ID (10.1.1.21) (Process ID 1)

                Router Link States (Area 400)

Link ID         ADV Router      Age         Seq#       Checksum Link count
10.1.1.17       10.1.1.17       330         0x80000016 0x00AF9B 1
10.1.1.21       10.1.1.21       109         0x80000010 0x001EF1 2
192.168.1.1     192.168.1.1     110         0x8000001B 0x00ACB9 3

                Net Link States (Area 400)

Link ID         ADV Router      Age         Seq#       Checksum
128.10.110.82   192.168.1.1     330         0x80000001 0x00936A
128.10.110.86   192.168.1.1     110         0x80000003 0x009F54

                Summary Net Link States (Area 400)

Link ID         ADV Router      Age         Seq#       Checksum
10.1.1.5        10.1.1.17       248         0x80000008 0x0025C1
10.1.1.9        10.1.1.17       248         0x80000006 0x0001E3
10.1.1.13       10.1.1.17       248         0x80000008 0x00D40A
10.1.1.17       10.1.1.17       248         0x80000008 0x007189
128.10.110.68   10.1.1.17       248         0x80000008 0x006C52
128.10.110.72   10.1.1.17       249         0x80000008 0x004476
128.10.110.76   10.1.1.17       249         0x80000008 0x001C9A

                Type-5 AS External Link States

Link ID         ADV Router      Age         Seq#       Checksum Tag
0.0.0.0         10.1.1.21       1385        0x80000007 0x004744 1
10.1.1.1        10.1.1.17       249         0x80000008 0x00A4B1 0
128.10.110.64   10.1.1.17       249         0x80000008 0x00F537 0
```

Figura 39 Base de datos Link-State-GYE.

Realizado por: *Morales, W. 2016.*

MENSAJES LSA

LSA TIPO 1

Todos los routers utilizan estos mensajes para describir y publicar sus redes, mediante este mecanismo OSPF construye su tabla topológica. Existen tres tipos de mensajes LSA de tipo 1:

- *Tipo Stub, el cual indica si existe una relación de vecindad con otro equipo, usado frecuentemente por Loopbacks.*
- *Tipo Transit, significa que el router en cuestión se encuentra ligado a un medio multi-acceso como Ethernet donde en teoría se podría establecer múltiples adyacencias. Es necesaria la elección de un DR-BDR.*
- *Tipo Point-Point, muestran el listado de routers vecinos en un enlace WAN.*

LSA TIPO 2

Describe la información en un segmento multi-acceso donde pueden estar conectados varios equipos. Este LSA solo lo usa el DR.

- *Los LSA tipo 1 y 2 tienen alcance de área, si es necesario pasar información sumarizada inter-área el router ABR debe usar LSAs tipo 3, quien tiene información tanto de las áreas en cuestión como Links-ID.*
- *Los LSA de este tipo muestra un listado con los Router-ID de todos los vecinos a través de una red multi-access, con estos mensajes se pueden descubrir todo el árbol topológico de la arquitectura.*

Los LSA's 1-2 viajarán por sus respectivas áreas desde los spokes (IMB, LJA, AMB) por medio de la nube Frame-Relay hacia el hub CCA. La ventaja de usar Frame-Relay con OSPF es que se podría usar cualquier tipo de red que ofrece OSPF, sin embargo en la mayoría de las implantaciones se opta por configurar una red NBMA, aunque se podría trabajar con una red tipo broadcast sin problemas.

Se debe tener en consideración que si se trabaja en una red tipo broadcast, al ser un medio multi-acceso en teoría se podrían formar múltiples adyacencias por lo que es necesario la elección de un Router Designado (DR) para que sea quién administre las adyacencias.

Si no se tuviera la elección de un router para administrar las vecindades, OSPF se vería en la necesidad cuando se ingrese un nuevo router a la topología, establecer adyacencias con todos los equipos del área sin excepción alguna. Esto a largo plazo no sería escalable puesto que disminuiría en ancho de banda de la red por la cantidad de LSAs y actualizaciones.

Con la siguiente estructura se podría llegar a calcular el número de adyacencias sin un DR:

$$\#Adyacencias = n(n-1)$$

Ecuación 3 Cálculo de adyacencias en redes tipo broadcast

Por ejemplo, si se tuviera 10 routers en una red tipo Broadcast se necesitarían formar 90 adyacencias; si entrara a la topología un router más, deberían formar 110 adyacencias. Esto hace que la red no sea escalable.

Otro problema que sucedería en redes de este tipo sin un DR, es que cuando un router envía una actualización o paquete al medio, los demás routers re-envían estos mensajes a todos los equipos aumentando de esta forma la cantidad de LSA's en la red.

OSPF ve la necesidad de escoger al Router Designado (DR) para que todo el resto de equipos de la red formen adyacencias completas con él y así reducir el número de adyacencias, es decir completarían el proceso de vecindad desde la Fase Down hasta la Fase Full donde los routers comparten la misma base de datos Link-State con su par. El BDR por su lado también forma adyacencias como si fuera un DR con el resto de equipos, si algo llegase a pasar con el DR el router BDR tomaría ese rol para no dejar incomunicada a la red.

Para tener la seguridad que si pasa algo con el DR no se caiga la red, OSPF busca mediante el algoritmo SPF un router que sirva de Backup (BDR) en caso que falle el DR. El resto de equipos que no son ni DRo BDR tienen la denominación de DROTHERs. Los DROTHERs envían cualquier tipo de mensaje o LSA hacia el DR usando la dirección multicast 224.0.0.5 con una frecuencia de 10 segundos en redes tipo Broadcast y cada 30 segundos en redes tipo Non Bradcast. Cuando el DR necesite enviar actualizaciones lo hará vía multicast usando la dirección 224.0.0.6.

En la práctica quién realmente se convierte en DR es el primer equipo que envíe LSA's 1-2 dentro del área, como no formaría una adyacencia con un vecino se autodenomina el Router Designado. Cuando otro router entra a la red, forma la adyacencia y durante ese proceso intercambia información quedando como el BDR. De ahí en adelante todo el resto de equipos que entre a la topología deberá ser DROTHERS aunque tengan mejores características como:

- *Priority*
- *Dirección de Loopback más alta*
- *IP de la interfaz física más alta*

Si se configura la nube Frame-Relay en conjunto con OSP para trabajar como red Punto-Multipunto se reducen significativamente las configuraciones, se envían paquetes Hello cada 10 segundos y su Hold time de 120 segundos. El problema que se presenta en este tipo de redes es que es necesario usar mappings para que un router tenga conectividad IP con los demás routers, los mappings indican a un router que DLCI deber usar para alcanzar a un vecino. En este caso la configuración es más compleja porque el router debe conocer todos los DLCI de sus vecinos.

```
CCA#sh ip ospf interface se 0/0/0.102
Serial0/0/0.102 is up, line protocol is up
  Internet Address 128.10.110.78/30, Area 100
  Process ID 1, Router ID 10.1.1.17, Network Type POINT_TO_POINT, Cost: 1562
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:03
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/6, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 3, maximum is 5
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.1.1.13
  Suppress hello for 0 neighbor(s)
IMB#sh ip ospf int se 0/0/0.201
Serial0/0/0.201 is up, line protocol is up
  Internet Address 128.10.110.77/30, Area 100
  Process ID 1, Router ID 10.1.1.13, Network Type POINT_TO_POINT, Cost: 1562
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:02
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 9/11, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 2, maximum is 2
  Last flood scan time is 0 msec, maximum is 4 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.1.1.17
  Suppress hello for 0 neighbor(s)
```

Figura 40 Interfaces OSPF-CCA, IMB.

Realizado por: *Morales, W. 2016.*

La topología Punto-Multipunto hace que se creen enlaces Punto-Punto entre el Hub (CCA) con el resto de Spokes (IMB, LJA, AMB) de manera que ya no se crean varios mappings para cada destino; sino solo 1 mapping apuntando como destino al Hub.

En otras palabras, si los spokes desean salir de su nube Frame-Relay será necesario únicamente apuntar al Hub (CCA) y éste router se encargará de direccionar el paquete fuera de la nube. El Hub siempre será el Next-Hop para todas las transmisiones.

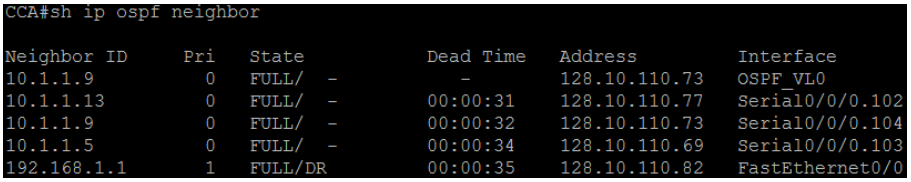
Todos los equipos que se encuentran dentro de la nube Frame-Relay tienen la misma configuración, usan al router CCA como punto de salida hacia otras redes.

```
FL#sh ip ospf interface fastEthernet 0/0
*Mar  1 00:31:49.651: %SYS-5-CONFIG_I: Configured from console by console
FL#sh ip ospf interface fastEthernet 0/0
FastEthernet0/0 is up, line protocol is up
  Internet Address 172.31.127.154/30, Area 0
  Process ID 1, Router ID 30.2.2.2, Network Type POINT_TO_POINT, Cost: 1
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:04
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 6, maximum is 7
  Last flood scan time is 0 msec, maximum is 4 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.2.1
  Suppress hello for 0 neighbor(s)
CA#sh ip ospf in fa 0/0
FastEthernet0/0 is up, line protocol is up
  Internet Address 172.31.127.149/30, Area 0
  Process ID 1, Router ID 30.5.5.5, Network Type POINT_TO_POINT, Cost: 1
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:01
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 3/3, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 5
  Last flood scan time is 0 msec, maximum is 4 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.2.1
  Suppress hello for 0 neighbor(s)
```

Figura 41 Interfaces OSPF-CCA, IMB.

Realizado por: *Morales, W. 2016.*

Las interfaces que une FL y CA se encuentran configuradas como Point-Point. Aunque sea un enlace multi-acceso donde se esperaría la elección de un DR para administrar las adyacencias configurado de esta forma y con los mismos timers la relación de vecindad se establece sin problemas.



```
CCA#sh ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.1.1.9          0   FULL/  -          -        128.10.110.73   OSPF_VL0
10.1.1.13         0   FULL/  -        00:00:31   128.10.110.77   Serial0/0/0.102
10.1.1.9          0   FULL/  -        00:00:32   128.10.110.73   Serial0/0/0.104
10.1.1.5          0   FULL/  -        00:00:34   128.10.110.69   Serial0/0/0.103
192.168.1.1       1   FULL/DR         00:00:35   128.10.110.82   FastEthernet0/0
```

Figura 42 Tabla de vecindad-CCA.

Realizado por: *Morales, W. 2016.*

LSA TIPO 3

LSA usado únicamente por ABRs, contienen información de enrutamiento cuando se necesita pasar información inter-áreas, tiene las siguientes características:

- *Toda la información enviada a otra área se encuentra sumarizada (Link ID de la red, máscara, métrica), de esta forma se sabe el costo total desde el ABR hacia un destino.*
- *El ABR publica de forma sumarizada a otras áreas el coste hacía sus redes internas, de esta forma si router fuera del área necesita acceder a ese destino deberá añadir su coste hacia el ABR. El router pensará que el destino se encuentra conectado directamente al ABR.*
- *Si existen varios ABR hacia un mismo destino, el origen escogerá al ABR que le ofrezca menor métrica. En resumen este LSA inyecta información de una área a otra.*

LSA TIPO 4-5

Estos LSAs sirven para publicar dominios externos a una red.

- *Los LSAs tipo 4 solo son usados por ABR, la información encontrada es la siguiente:*
  - *Máscara (ASBR) , link-state (red)*
  - *Métrica*
  - *Router ID (ABR)*
- *Los LSAs tipo 5 solo son usados por ASBR, la información encontrada es la siguiente:*
  - *Link ID (red externa), máscara*
  - *Métrica*
  - *Router ID (ASBR)*

- *Como los ABR limitan el paso de LSA1-2 a otras áreas, y LSAs 3 solo muestran información de Links-ID disponibles, hacen necesario LSA tipo 4-5 para definir el mecanismo de llevar información extra.*
- *Los LSA tipo 4 muestra información del costo hacia el ASBR (Sumarizada)*
- *Los LSA tipo 5 muestran información del costo hacia una ruta externa, de esta forma este tipo de LSA publica la métrica externa y los ABR ayudar a descifrar la métrica para llegar al ASBR para tener una métrica total hacia un destino fuera del ASBR.*

LSA TIPO 7

Ya que no es permitido el paso de LSA 4-5 en redes tipo NSSA, este tipo de LSA 7 es usado únicamente por ASBR, sirven para inyectar rutas externas. Tienen una estructura similar a LSAs tipo 5:

  - *Router ID (ASBR, quien inyecta la ruta)*
  - *Link ID, máscara*
  - *Métrica*
- *Cuando un router quiere salir a una red externa, usa LSAs tipo 3 para calcular la métrica hasta el ABR más cercano, éste ABR al saber la métrica hasta el ASBR envía la información por la interfaz adecuada y el ASBR envía el paquete el exterior del área.*

$$Métrica = Coste\ hacia\ ABR + coste\ a\ interfaz\ de\ ASBR + coste\ publicado\ por\ ASBR$$

Ecuación 4 Métrica OSPF para redes externas redistribuidas

```
IMB#sh ip ospf database

           OSPF Router with ID (10.1.1.13) (Process ID 1)

               Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
10.1.1.13       10.1.1.13       114         0x80000002 0x00CD40 0

               Router Link States (Area 100)

Link ID         ADV Router      Age         Seq#       Checksum Link count
10.1.1.13       10.1.1.13       114         0x80000003 0x007167 3
10.1.1.17       10.1.1.17       103         0x80000003 0x0028D4 2

               Summary Net Link States (Area 100)

Link ID         ADV Router      Age         Seq#       Checksum
10.1.1.5        10.1.1.17       103         0x80000002 0x00D610
10.1.1.9        10.1.1.17       103         0x80000002 0x00AE34
10.1.1.17       10.1.1.17       103         0x80000002 0x0023D7
10.1.1.21       10.1.1.17       1859        0x80000001 0x006B81
128.10.110.68   10.1.1.17       103         0x80000002 0x001EA0
128.10.110.72   10.1.1.17       103         0x80000002 0x00F5C4
128.10.110.80   10.1.1.17       1854        0x80000003 0x00725E
128.10.110.84   10.1.1.17       1861        0x80000001 0x00B212
192.168.1.0     10.1.1.17       1808        0x80000001 0x001193

               Type-7 AS External Link States (Area 100)

Link ID         ADV Router      Age         Seq#       Checksum Tag
10.1.1.1        10.1.1.13       116         0x80000002 0x003422 0
128.10.110.64   10.1.1.13       116         0x80000002 0x0085A7 0

               Router Link States (Area 200)

Link ID         ADV Router      Age         Seq#       Checksum Link count
10.1.1.13       10.1.1.13       116         0x80000002 0x00CD40 0

               Type-5 AS External Link States

Link ID         ADV Router      Age         Seq#       Checksum Tag
10.1.1.1        10.1.1.13       116         0x80000002 0x008AEE 0
128.10.110.64   10.1.1.13       116         0x80000006 0x00D378 0
```

Figura 43 Base de datos Link-State-IMB.

Realizado por: *Morales, W. 2016.*

- *Los LSA tipo 7 son traducidos a LSA 5 por los ABR, si hay varios se utiliza el equipo con el Router-ID más alto indicando el forward address como destino para alcanzar el ASBR. Se recomienda utilizar una dirección de Loopback como forward address, ya que esta dirección de Loopback forma parte de la red NSSA. Si no existe ésta, se escogerá una dirección física como válida. Con esto se puede concluir que un LSA tipo 7 es un LSA tipo 5 con un forward address.*

OSPF tiene la posibilidad de manejar diversas áreas dentro del AS100, por lo que ayuda a mejorar el desempeño de la red notablemente ya que cada área maneja una Base de Datos Link-State distinta y esto repercute al tiempo de convergencia de cada una de las áreas. Si un prefijo de red desaparece de una base de datos de una determinada área, Dijkstra re-calcula

todas las rutas de ese proceso mediante LSA 1-2 y envía las respectivas actualizaciones a otras áreas usando LSA 3.

Cuando se tiene una área con muchos equipos se ve la necesidad de dividir la topología en varias ´Islas" independientes creando una subdivisión del dominio de enrutamiento de OSPF, ya que por cada cambio topológico se re-calcularán las rutas haciendo que las actualizaciones consuman ancho de banda y demás recursos de la red.

Otro problema de mantener una sola área para toda la arquitectura de red, es que el algoritmo SPF correrá cada vez que haya un cambio en la topología y como todos los equipos deben tener la misma tabla de rutas mayor será el tiempo de consolidación de dicha tabla haciendo que la red converja de forma lenta. Además que mientras siga creciendo la red, mayor será la cantidad de rutas que compartan los equipos haciendo que la búsqueda de una ruta sea cada vez más compleja, afectando a la latencia de la red, paquetes perdidos y a causa de eso información erróneo en la base de datos.

OSPF tiene la necesidad que todos los equipos que forman parte del área compartan la misma información de enrutamiento, por lo que mantener ese esquema no es una solución escalable. La solución a este problema es que se divida la topología en diversas áreas, este mecanismo asegura que la red sea de fácil administración, escalable y convergencia rápida; aprovechando el recurso más valioso de una red, el ancho de banda.

El AS 100 tiene diversos tipos de áreas que facilitan la convergencia de enrutamiento, entre ellas se tiene:

AREA DE BACKBONE

- *Al manejar OSFP varios áreas y de alguna manera segmentar la red en "islas más pequeñas" da la posibilidad de construir escalable.*
- *El algoritmo SPF funciona de manera independiente en cada área*

- *Todas las áreas están conectadas físicamente al backbone, por esta razón esta área debe tener mayor redundancia mediante el uso de virtual-links, ya que si ésta falla también sus LSAs y por ende toda la red no tendrá conectividad.*
- *Todos los anuncios entre áreas pasan obligatoriamente por su backbone, haciendo notable que no pueden haber 2 ó más áreas.*

AREA REGULAR

- *Son usadas con el fin de limitar y reducir las publicaciones de LSA 1-2, ayudando a la reducción de uso de CPU y memoria de routers.*

ÁREA STUB

- *No se permiten LSA 4-5, por lo que no están permitidos ASBRs que son quienes lo pueden generar.*
- *Los ABR inyectan LSA 3 al área Stub*
- *No está permitido la inyección de información de otros AS a estas áreas.*
- *Los routers que se encuentran dentro de esta área no necesitan tener conexión directa con las rutas externas ya que de esta función se encarga el ASBR ya que ellos inyectan información con las rutas que se encuentran fuera del AS.*

AREA TOTALLY STUB

- *No se permiten LSA tipo 3, 4, 5*
- *Los routers ABR conocen como llegar a rutas externas*
- *No se aceptan rutas inter área (entre áreas), es decir no se permiten rutas externas en el interior de esta área. Por lo contrario si se aceptan rutas intra área (dentro del área)*

AREA NSSA

- *Son muy parecidas a las redes tipo Stub, con la diferencia que estas áreas sí soportan routers ASBRs con el fin de inyectar rutas externas a la red pero sin usar LSA tipo 5. En*

su lugar se usan LSA tipo 7 para que el área NSSA tenga conocimiento de salir hacia rutas externas.

- *El ABR tiene la tarea de traducir LSA 5 a LSA 7 cuando un router que pertenece al área NSSA desea tener comunicación con rutas externas.*
- *Esta área se comunica con su backbone a través de LSA tipo 3*
- *El ABR no inyecta al interior de áreas NSSA rutas por defecto*

TOTALLY STUB (AREAS NO SUMMARY)

- *No permiten la generación de LSA tipo 3, 4, 5*
- *Se permite la generación de rutas por defecto con el fin de poderse comunicar con ASBRs de otras áreas, cuando el ASBR inyecta rutas al interior del área utilizan LSA tipo 7 y los ABR con el Router-ID más altos traducen a LSAs tipo 5 para que los routers ABR de otras áreas conozcan cómo llegar a su respectivo ASBR.*

VIRTUAL LINKS

Los virtual links ayudan a resolver problemas de conectividad cuando se presentan malos diseños topológicos, es necesario acudir a este mecanismo cuando se tiene los siguientes escenarios:

- *Cuando una determinada área no tiene conexión física con el área de backbone.*
- *Cuando se particiona el área 0*
- *Cuando es necesario unir 2 redes OSPF distintas.*

```
CCA#sh ip ospf virtual-links
Virtual Link OSPF_VL0 to router 10.1.1.9 is up
  Run as demand circuit
  DoNotAge LSA allowed.
  Transit area 200, via interface Serial0/0/0.104, Cost of using 1562
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:07
    Adjacency State FULL (Hello suppressed)
    Index 1/4, retransmission queue length 0, number of retransmission 1
    First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
    Last retransmission scan length is 1, maximum is 1
    Last retransmission scan time is 0 msec, maximum is 0 msec
```

Figura 44 Virtual-Link-CCA.

Realizado por: *Morales, W. 2016.*

Para áreas que no se encuentran físicamente conectadas al área de backbone y que no intercambian LSAs de ningún tipo, se debe tener en cuenta que las áreas conectadas por un Virtual-Link no deben ser áreas tipo Stub ni áreas tipo NSSA.

Otro factor a tener en consideración es que la métrica asociada entre los ABR de las áreas no debe exceder de 65535.

El AS100 posee un Virtual-Link entre el router CCA y LJA quienes serían los dos ABRs que realicen la conexión, el área 200 servirá de puente de conexión entre el área de backbone y el área 500 que no tiene conexión física hacia ella. El router CCA permitirá el intercambio de la base de datos topológica completa entre las áreas en cuestión.

Los virtual-Links no deben ser considerados dentro del diseño de una red, sino más bien como un mecanismo de emergencia en los siguientes casos:

- *Fractura del Área 0*
- *Fusión de 2 empresas que manejen OSPF*
- *Redundancia en áreas críticas*

AUTENTICACION

El proceso de autenticación en OSPF ayuda a validar la adyacencia de vecindad entre equipos, además de garantizar que dicha asociación se produzca entre equipos autorizados ganando de esta forma ataques de hacking como "Man in the middle".

TIPOS:

- *NULL (Tipo 0).- No existe ningún tipo de autenticación, por lo que se permite la asociación de cualquier dispositivo en el área.*

- *SIMPLE (Tipo 1).- Es necesario para que los dispositivos establezcan una adyacencia manejen el mismo tipo de autenticación, en este tipo de método la información y la clave viaja en texto plano.*
- *MD5 (Tipo 2).- Ambos equipos deben compartir su hash y clave, este tipo de mecanismo usa un proceso criptográfico donde la clave entra a un algoritmo matemático y es transformado en un hash. Cada equipo calcula su propio hash, con lo cual al final el password encriptado deben coincidir en ambos equipos.*

Si dos equipos se encuentran asociados a través de una autenticación md5 y posteriormente uno de los ellos cambia su key o password, la adyacencia no se perderá. Pues hasta que del otro lado remoto no se configure con la misma información, no caerá la vecindad. Con esto se evita que caiga la relación cuando se modifica la autenticación.

5.2.3.Protocolo de enrutamiento ISIS

- *Fue desarrollado por OSI conjuntamente con OSPF para ser la competencia de TCP/IP*
- *Los datos son encapsulados a nivel de enlace de datos, además que el modelo de enrutamiento es transparente ya que puede trabajar con IPv4 e IPv6.*
- *Maneja un modelo propio de direccionamiento llamado Connection Less Network(CLNS):*
    - *Level 0: Usado para dispositivos finales como host-routers (usado en hasta hace unos años)*
    - *Level 1: Enrutamiento intra-área*
    - *Level 2: Enrutamiento inter-áreas*
    - *Level 3: Enrutamiento entre dominios (Ahora remplazado por BGP)*
- *Tipos de routers:*
    - *Level 1: Dispositivos los cuales enrutan paquetes intra-área*
    - *Level 2: Dispositivos de borde donde el equipo pertenece a una determinada área.*

- *Basado en Link-State y el algoritmo matemático Dijkstra*
- *Métrica basada en throughput, no en ancho de banda.*
- *IS-IS fue diseñado para trabajar en redes tipo backbone, en casos especiales su desempeño es mejor que OSPF. El backbone es la consecución de enlaces L2, el cual se partiría si la consecuencia de dichos enlaces es interrumpido cuando atraviesa un enlace L1*
- *Las redes soportadas por IS-IS pueden ser de tipo broadcast (LAN, Multipunto: Frame-Relay, ATM). Además es necesario escoger un Router Designated (DIS) el cual escogido por su prioridad (métrica), es el encargado de administrar y anunciar todos los cambios topológicos del área. Para la elección del DIS se debe tener en cuenta:*
    - *Prioridad más alta*
    - *Dirección MAC más alta*

Una vez que la adyacencia se haya formado cada router envía su LSP conteniendo toda la información de las redes que se tiene conectado. El DIS recolecta toda esa información y lo envía usando mensajes CSNP (Complete Secuence Number PDU), el cual contiene todos los LSP de los neighbors dentro del área. Solo el DIS envía mensajes de este tipo con un rango de frecuencia de 10 segundos.

En una red tipo Point-Point no tiene sentido que exista un DIS puesto que ninguno de los equipos administrará adyacencias para otros routers; cuando un router necesita información sobre alguna ruta simplemente envía un mensaje PSNP. En este caso cuando los routers levantan la adyacencia se envían mensajes CSNO conteniendo todos los LSPs que mantienen cada uno por su lado.

Un aspecto importante del protocolo de enrutamiento IS-IS, es que ninguna de las interfaces de un equipo posee direccionamiento IP ya que la red representa a todo el equipo, no a interfaces.

IS-IS maneja preferencia de rutas según el nivel:

- *L1*
- *L2*
- *Externas*

IS-IS maneja tipos de timers:

Los mensajes Hello en routers que no sean DIS se dan cada 10 segundos, mientras que en routers DIS es de cada 3.3 segundos. El Hold time es por defecto 3 veces el tiempo de Hello, es decir 30 segundos y 9.9 segundos respectivamente.

- *Hello en redes Multi-acceso:*

  Para mensajes Hello en routers de Nivel 1 se utiliza como dirección multicast de destino 01:80:C2:00:00:14

  Para mensajes Hello en routers Nivel 2 se utiliza como dirección multicast de destino 01:80:C2:00:00:15

```
NY#sh clns neighbors detail

System Id      Interface   SNPA            State  Holdtime  Type Protocol
FL             Se0/0/0     *HDLC*          Up     21        L2   IS-IS
  Area Address(es): 49.0015
  IP Address(es):  172.31.127.137*
  Uptime: 05:25:55
  NSF capable
TX             Se0/1/0     *HDLC*          Up     23        L2   IS-IS
  Area Address(es): 49.0015
  IP Address(es):  172.31.127.141*
  Uptime: 05:55:10
  NSF capable
```

Figura 45 Tabla de vecindad-NY.
Realizado por: *Morales, W. 2016.*

- *Hello en Redes Point-Point:*

  Existe un solo tipo de Hello para todos los routers tanto de Nivel 1 como Nivel 2

  Para establecer adyacencias los routers deben estar en la fase de 2 Init.

  Si un router es L1 significa que es un router interno, mientras que si el router es de Nivel 2 podrá comunicarse con routers de distintas áreas. Este tipo de router puede

hacer redistribución de rutas con otros protocolos de enrutamiento. Además de usar direccionamiento multicast para enviar actualizaciones.

- *LSP (Link-State Packet):*

  Cuando un router activa en su cabecera el bit ATT significa que ese router puede servir como un default Gateway para que los routers de Nivel 1 puedan alcanzar áreas externas. Cuando un router interno se da cuenta que algún vecino tiene activo el ATT sabrá que puede alcanzar rutas externas por ese equipo.

  IS-IS reconoce de forma automática las vecindades asociando el hostname del router más su System-ID; Dijkstra busca en los TLVs la información para crear la base de datos topológica para luego hacer la tabla de rutas escogiendo las mejores métricas para alcanzar a los destinos.

  CSNP (Link-State Packet):

  Contiene informacion sumarizada de todas las rutas que se tiene, basada en esta información un router será capaz de reconocer si le hace falta alguna ruta en su base de datos, si es así podrá pedir la actualización a su vecino DIS. En redes multi-acceso solo el DIS es quien envía CSNPs cada 10 segundos. En redes Point-Point ambos routers envían CSNPs cada 10 segundos.

```
TX#sh clns neighbors detail

System Id      Interface   SNPA            State  Holdtime  Type Protocol
FL             Se0/0       *HDLC*          Up     24        L1   IS-IS
  Area Address(es): 49.0015
  IP Address(es):  172.31.127.133*
  Uptime: 05:17:08
  NSF capable
NY             Se0/1       *HDLC*          Up     29        L2   IS-IS
  Area Address(es): 49.0020
  IP Address(es):  172.31.127.142*
  Uptime: 05:45:33
  NSF capable
```

Figura 46 Tabla de vecindad-NY.
Realizado por: *Morales, W. 2016.*

- *PSNP:*

  Sirven para confirmar mensajes LSPs así como para pedir información a vecinos cuando un router interno recibe un CSNP y le hace falta una ruta; en ese instante envía un mensaje PSNP para pedir un envío de la ruta faltante o si es necesario todo el LSP.

Dos routers pueden levantar adyacencias sin importar el tipo de timers que manejen, se puede tener el caso que una red multiacceso puede tener configurado el CSNP en cada interfaz de forma distinta incluso para cada segmento de red y la adyacencia se podría levantar sin problemas.

```
FL#sh clns neighbors detail

System Id      Interface   SNPA            State  Holdtime  Type Protocol
TX             Se0/0       *HDLC*          Up     24        L1   IS-IS
  Area Address(es): 49.0015
  IP Address(es):  172.31.127.134*
  Uptime: 00:41:25
  NSF capable
NY             Se0/1       *HDLC*          Up     28        L2   IS-IS
  Area Address(es): 49.0020
  IP Address(es):  172.31.127.138*
  Uptime: 00:40:35
  NSF capable
```

Figura 47 Tabla de vecindad-FL.

Realizado por: *Morales, W. 2016.*

Se debe tener en consideración en el diseño de una red que en redes Point-Point no existe un DIS, así como cuando hay dos routers formando parte de una L2 los routers comparten la misma Base de Datos. Todos los routers L1 comparten la misma Base de Datos. Por otro lado cuando no existe un DIS dentro de la topología el Circuit-ID en los routers es de 0; si e=n ese campo se tiene un valor diferente de 0 y es una interfaz L2, no se levanta la relación de vecindad.

El DIS en una red tipo Broadcast es el encargado de anunciar mensajes CSNP; para escoger el DIS se debe tener en consideración las siguientes prioridades:

- *Comando: Priority*
- *Coste de sus interfaces*
- *MAC Address*

Las interfaces de un router en una red tipo Broadcast es de 64

No es una restricción para IS-IS que los routers que formen la adyacencia tengan timers distintos

```
NY#sh isis hostname
Level  System ID      Dynamic Hostname  (notag)
 2     0300.0200.2002 FL
 2     0300.0300.3003 TX
     * 0300.0400.4004 NY
TX#sh isis hostname
Level  System ID      Dynamic Hostname  (notag)
 1     0300.0200.2002 FL
     * 0300.0300.3003 TX
 2     0300.0400.4004 NY
FL#sh isis hostname
Level  System ID      Dynamic Hostname  (notag)
     * 0300.0200.2002 FL
 1     0300.0300.3003 TX
 2     0300.0400.4004 NY
```

Figura 48 Hostname NY, TX, FL.

Realizado por: *Morales, W. 2016.*

IS-IS maneja los siguientes tipos de paquetes:

- *CSNP.- Recoge informacion de todos los LSPs haciendo un resumen de la Base de Datos que se envían cada 10 segundos.*
- *LSP Life Time.- Es el tiempo de validez de un LSP, se envían cada 1200 segundos. Durante este tipo la informacion de direccionamiento es válido.*
- *LSP Refresh.- Tiempo en el cual se re-envían los LSP, por defecto es cada 900 segundos.*
- *LSP Interval.- Es el intervalo entre mensajes LSP, se dan cada 33 ms. Cuando existen muchos LSPs no se envían todos al mismo tiempo, los mensajes se ponen en cola teniendo un intervalo entre ellos de 33ms.*
- *LSP Retransmit.- IS-IS asegura que todos los LSPs deben ser configurados para que envíen un Acknowledgement (ACK) como respuesta de recepción, si durante 5 segundos no llega un ACK como respuesta se deberá volver a re-enviar el mensaje.*

```
NY#sh ip route isis
     172.31.0.0/16 is variably subnetted, 9 subnets, 3 masks
i L2    172.31.127.132/30 [115/20] via 172.31.127.141, Serial0/1/0
                          [115/20] via 172.31.127.137, Serial0/0/0
i L2    172.31.127.128/30 [115/20] via 172.31.127.137, Serial0/0/0
i L2    172.31.127.152/30 [115/20] via 172.31.127.137, Serial0/0/0
i L2    172.31.127.148/30 [115/20] via 172.31.127.137, Serial0/0/0
i L2    172.31.127.144/30 [115/20] via 172.31.127.137, Serial0/0/0
i L2    172.31.122.0/23 [115/20] via 172.31.127.137, Serial0/0/0
i L2 192.168.2.0/24 [115/20] via 172.31.127.137, Serial0/0/0
     30.0.0.0/32 is subnetted, 5 subnets
i L2    30.5.5.5 [115/20] via 172.31.127.137, Serial0/0/0
i L2    30.2.2.2 [115/10] via 172.31.127.137, Serial0/0/0
i L2    30.3.3.3 [115/10] via 172.31.127.141, Serial0/1/0
i L2    30.1.1.1 [115/20] via 172.31.127.137, Serial0/0/0
```

Figura 49 Tabla de enrutamiento-NY.

Realizado por: *Morales, W. 2016.*

Existen paquetes que se envían entre routers, así como entre routers y dispositivos finales, esto puede ser observado en la cabecera del protocolo donde:

- *0x83.- Significa que los paquetes intercambiados fueron entre routers.*
- *0x82.- Significa que los paquetes intercambiados fueron entre routers y dispositivos finales*

```
FL#sh ip route isis
     172.31.0.0/16 is variably subnetted, 9 subnets, 3 masks
i L1    172.31.127.140/30 [115/20] via 172.31.127.134, Serial0/0
i L2    172.31.127.0/26 [115/20] via 172.31.127.138, Serial0/1
     30.0.0.0/32 is subnetted, 5 subnets
i L2    30.4.4.4 [115/10] via 172.31.127.138, Serial0/1
i L1    30.3.3.3 [115/10] via 172.31.127.134, Serial0/0
```

Figura 50 Tabla de vecindad-FL.

Realizado por: *Morales, W. 2016.*

IS-IS maneja los siguientes tipos de PDUs:

- *LSP.- El cual lleva informacion de enrutamiento interno*
- *PSNP (Partial Secuence Number PDU).- Sirven para confirmar la recepción de un LSP y también para entregar informacion de un LSP hacia un vecino*
- *CSNP (Complete Secuence Number).- Muestra un resumen de la Base de Datos donde se muestran todos los LSP internos.*

```
TX#sh ip route isis
     172.31.0.0/16 is variably subnetted, 9 subnets, 3 masks
i L1    172.31.127.136/30 [115/20] via 172.31.127.133, Serial0/0
i L1    172.31.127.128/30 [115/20] via 172.31.127.133, Serial0/0
i L1    172.31.127.152/30 [115/20] via 172.31.127.133, Serial0/0
i L1    172.31.127.148/30 [115/20] via 172.31.127.133, Serial0/0
i L1    172.31.127.144/30 [115/20] via 172.31.127.133, Serial0/0
i L1    172.31.122.0/23 [115/20] via 172.31.127.133, Serial0/0
i L2    172.31.127.0/26 [115/20] via 172.31.127.142, Serial0/1
i L1 192.168.2.0/24 [115/20] via 172.31.127.133, Serial0/0
     30.0.0.0/32 is subnetted, 5 subnets
i L2    30.4.4.4 [115/10] via 172.31.127.142, Serial0/1
i L1    30.5.5.5 [115/20] via 172.31.127.133, Serial0/0
i L1    30.2.2.2 [115/10] via 172.31.127.133, Serial0/0
i L1    30.1.1.1 [115/20] via 172.31.127.133, Serial0/0
```

Figura 51 Tabla de vecindad-NY.

Realizado por: *Morales, W. 2016.*

5.2.4.Protocolo de enrutamiento BGP

Border Gateway Protocol es un protocolo EGP que no tiene convergencia rápida, sin embargo su objetivo de no es llevar información que tiene que ver con los protocolos IGP los cuales sí tienen convergencia rápida, sino más bien manejar grandes tablas de enrutamiento y con llevar

prefijos de clientes desde y hacia el backbone de Internet. BGP se define como un protocolo que implementa políticas de enrutamiento, funciona sobre TCP y delega toda la función de re transmisiones, control de errores y flujo al stack TCP; a diferencia de los protocolos IGP los cuales si dedican procesamiento a esos detalles. BGP se concentra y pone todo su procesamiento en enrutar paquetes entre Sistemas Autónomos.

BGP es un protocolo que no está orientado al manejo de métricas sino más bien en atributos de prefijos basados en Path-Vector, es decir cuenta el número de saltos entre sistemas autónomos lo cual le permite ir recogiendo información al respecto durante su paso para evitar loops. El protocolo permite su expansión a través de capabilities las cuales le permiten entre otras cosas filtrar rutas y alterar el tráfico de upstream como downstream.

BGP usa mensajes de tipo:

- *Open.- Mensajes enviados hacia otros routers que contienen información como Hold time, capabilities, identificador de AS y versión (IPv4, IPv6).*
- *Keep-alive.- Sirven para mantener vivas las conexiones mediante una marca de 16 bytes.*
- *Notificaciones.- Mensajes que indican errores en headers, mensajes open y actualizaciones antes de cerrar conexiones como por ejemplo cuando se detecta inconsistencias de AS.*
- *Updates.- Contienen información de los atributos o capabilities de BGP.*

5.2.4.1. Establecimiento de sesiones

Para que se establezca la relación de peering entre dos routers es necesario el establecimiento de una conexión TCP la cual servirá en lo posterior para hacer una comunicación bidireccional entre los vecinos. Durante esta etapa hay un cliente y un servidor, donde por lo general éste último debe mantener abierto el puerto TCP 179.

El router quien negocia como cliente establece la sesión usando un puerto mayor a 1024 con un destino 179. Si existe una colisión o ambos routers inician la conexión al mismo tiempo, el router que iniciará la sesión TCP será quien tenga el Router-ID más alto

5.2.4.2. Estados

Idle.- No se acepta ninguna conexión

Connect.- Se realiza un handshake y se envía un mensaje Open, durante este tiempo se debe enviar 3 keep-alives por cada Hold time.

Confirm.- Se comprueba si el router está de acuerdo con las capabilities enviadas. Se envían keep-alives para notificar al vecino que está de acuerdo con las capabilities.

- *Established.- Intercambian paquetes update*

5.2.4.3. Atributos

BGP posee ciertos mecanismos para realizar políticas de enrutamiento, existen dos clases de atributos:

- ***Mandatorios.-*** *Son obligados a reconocer por todos los routers, se encuentran dentro de mensajes Update. Ejemplos: ASPath, Origin y Next-Hop*
- ***Transitorios.-*** *Atributos que pueden o no ser leídos por un vecino, si bien es cierto un router no está en la obligación de leerlo pero si no lo hacen deben pasarlo a su vecino. Ejemplos: Aggregator, Community.*
- ***Discrecionarios.-*** *Si un router lo envía a otro, éste está obligado a leerlo. Ejemplos: Local-Preference, Attomic agregate.*
- ***No transitivos.-*** *El router no está en la obligación de pasarlo a su vecino. Ejemplos: MED, Originator ID, Cluster ID. Si el router entiende este atributo, no le envía a su vecino*

5.2.4.4. Capabilities

BGP negocia las capacidades que tendrá el router al inicio de la conexión BGP, el router que inicia primero la sesión y envía el mensaje Open, dentro del mensaje se encuentran todas las capabilities que soporta dicho equipo. Una vez compartida las capabilities entre los equipos pueden seguir extendiéndolas dependiendo del fabricante. Los tipos de capabilities soportadas:

- *IPv4*
- *Unicast*
- *Route-Refresh*

Cuando un router analiza las capabilities que le envía un vecino, aceptará solamente las cuales soporta; cuando su peer verifica que no soporta esa alguna ya no le enviará en el futuro.

```
GYE#sh ip bgp
BGP table version is 174, local router ID is 10.1.1.21
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.1/32      128.10.110.86           20         32768 ?
*> 10.1.1.5/32      128.10.110.86         1574         32768 ?
*> 10.1.1.9/32      128.10.110.86         1574         32768 ?
*> 10.1.1.13/32     128.10.110.86         1574         32768 ?
*> 10.1.1.17/32     128.10.110.86           12         32768 ?
*> 10.1.1.21/32     0.0.0.0                  0         32768 ?
*> 10.1.10.0/24     128.10.110.86         1574         32768 i
*> 30.1.1.1/32      200.1.1.2                      50      0 300 400 400 400 400 400 400 ?
*> 30.2.2.2/32      200.1.1.2                      50      0 300 400 400 400 400 400 400 ?
*> 30.3.3.3/32      200.1.1.2                      50      0 300 400 400 400 400 400 400 ?
*> 30.4.4.4/32      200.1.1.2                      50      0 300 400 400 400 400 400 400 ?
*> 30.5.5.5/32      200.1.1.2                      50      0 300 400 400 400 400 400 400 ?
   Network          Next Hop            Metric LocPrf Weight Path
r>i128.10.105.0/24  10.1.1.13                0    100      0 i
*> 172.31.122.0/23  200.1.1.2                      50      0 300 400 400 400 400 400 400 i
*> 172.31.127.0/26  200.1.1.2                      50      0 300 400 400 400 400 400 400 i
*> 192.168.1.0      128.10.110.86           11         32768 i
*> 192.168.2.0      200.1.1.2                      50      0 300 400 400 400 400 400 400 i
```

Figura 52 Tabla RIB-GYE.

Realizado por: *Morales, W. 2016.*

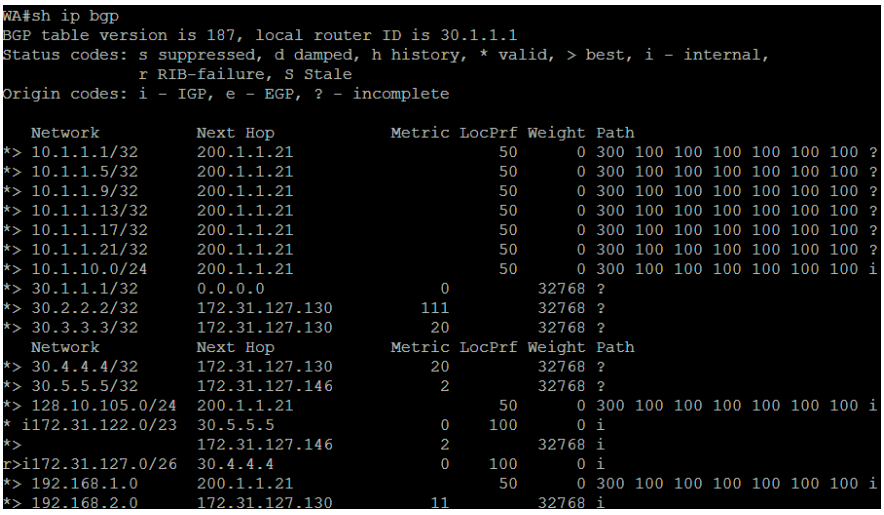
El parámetro Weight es usado para modificar las decisiones que usa BGP al momento de escoger las rutas hacia los destinos; como este valor tiene validez de forma local, todas las redes del AS400 tienen un valor de [0]. Se ha dejado configurado el valor por defecto [32768] como el peso que tendrán las rutas.

El parámetro AS_PATH recopila información mientras pasa por los diferentes AS con el fin de evitar loops de enrutamiento por haber pasado anteriormente por dichos AS. Como se puede observar las mejores rutas ingresan en la tabla RIB. Para alcanzar a cualquier vecino iBGP se

lo puede alcanzar por la interfaz Outside el firewall ASA1 [128.10.110.86], y si éstos desean salir del AS100, lo deberán hacer por GYE por el uso del Local Preference. Para alcanzar rutas del AS400.

Se puede observar que el número interno de la versión de la tabla es 174, este valor se incrementa cuando existe un cambio topológico. El Router-ID o BGP-ID es la dirección de Loopback 10.1.1.21. Se puede observar que todas las rutas hacia los iBGP han sido redistribuidas por algún protocolo en BGP. También se puede notar que la IP de la interfaz activa del ASA1, así como la red de la DMZ ha sido publicada usando el comando network.

Otra información importante es que la dirección de Loopback 10.1.1.21 ha sido auto originada, esto se puede notar ya que es el primer vecino externo en el camino así como por la dirección 0.0.0.0.



```
WA#sh ip bgp
BGP table version is 187, local router ID is 30.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.1/32      200.1.1.21                50      0 300 100 100 100 100 100 100 ?
*> 10.1.1.5/32      200.1.1.21                50      0 300 100 100 100 100 100 100 ?
*> 10.1.1.9/32      200.1.1.21                50      0 300 100 100 100 100 100 100 ?
*> 10.1.1.13/32     200.1.1.21                50      0 300 100 100 100 100 100 100 ?
*> 10.1.1.17/32     200.1.1.21                50      0 300 100 100 100 100 100 100 ?
*> 10.1.1.21/32     200.1.1.21                50      0 300 100 100 100 100 100 100 ?
*> 10.1.10.0/24     200.1.1.21                50      0 300 100 100 100 100 100 100 i
*> 30.1.1.1/32      0.0.0.0                    0          32768 ?
*> 30.2.2.2/32      172.31.127.130           111         32768 ?
*> 30.3.3.3/32      172.31.127.130            20         32768 ?
   Network          Next Hop            Metric LocPrf Weight Path
*> 30.4.4.4/32      172.31.127.130            20         32768 ?
*> 30.5.5.5/32      172.31.127.146             2         32768 ?
*> 128.10.105.0/24  200.1.1.21                50      0 300 100 100 100 100 100 100 i
* i172.31.122.0/23  30.5.5.5                   0    100      0 i
*>                  172.31.127.146             2         32768 i
r>i172.31.127.0/26  30.4.4.4                   0    100      0 i
*> 192.168.1.0      200.1.1.21                50      0 300 100 100 100 100 100 100 i
*> 192.168.2.0      172.31.127.130            11         32768 i
```

Figura 53 Tabla RIB-WA.

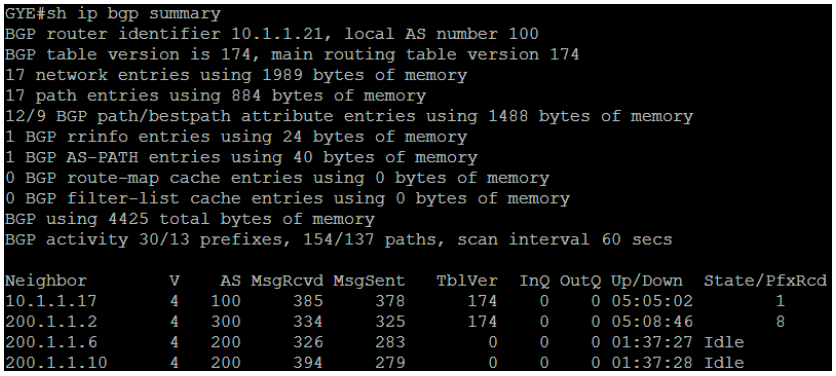
Realizado por: *Morales, W. 2016.*

El parámetro Local Preference es uno de los más importantes y usados en el presente caso de estudio, ya que ayuda a influir el tráfico dependiendo del valor que se maneje; en este caso sirve para indicarle al router WA por donde enviar el tráfico de upstream o "La salida preferida". Como este parámetro no transita entre sistemas autónomos, servirá para enrutar información a los peers iBGP del AS400. En el escenario que se llegase a necesitar que este parámetro transite por otros AS, será necesario implementar Confederaciones lo cual ya no es

usado con frecuencia en la actualidad ya que si el AS400 no fuera un AS público sería necesario la concesión de un AS privado por parte de un ISP o Tier 1, después de lo cual se tendría que implementar pequeños sistemas autónomos privados dentro del concesionado.

En este escenario cuando el router que está en otro AS recibe el Local Preference remoto, éste configurará localmente su Local Preference que le anuncia su peer. Con esta configuración todos los peers iBGP preferirán salir a dicho AS usando el router que recibió ese anuncio de confederaciones.

Cuando se configura BGP con el valor de Local Preference por defecto como en este caso, se anuncia a los iBGP que para salir del AS400 deben enrutar el tráfico hacia WA.



```
GYE#sh ip bgp summary
BGP router identifier 10.1.1.21, local AS number 100
BGP table version is 174, main routing table version 174
17 network entries using 1989 bytes of memory
17 path entries using 884 bytes of memory
12/9 BGP path/bestpath attribute entries using 1488 bytes of memory
1 BGP rrinfo entries using 24 bytes of memory
1 BGP AS-PATH entries using 40 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 4425 total bytes of memory
BGP activity 30/13 prefixes, 154/137 paths, scan interval 60 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.1.1.17       4   100     385     378      174    0    0 05:05:02        1
200.1.1.2       4   300     334     325      174    0    0 05:08:46        8
200.1.1.6       4   200     326     283        0    0    0 01:37:27 Idle
200.1.1.10      4   200     394     279        0    0    0 01:37:28 Idle
```

Figura 54 Tabla BGP-GYE.

Realizado por: *Morales, W. 2016.*

Se puede observar el estado de las sesiones de BGP y también el número de prefijos aprendidos en cada sesión; se puede observar que se tiene 17 entradas en la tabla RIB las cuales son IPv4 y provienen de AS como 100, 200, 300. Se puede conocer que por el AS 300 (R2-ISP1) el router GYE ha aprendido 8 prefijos de clientes y por el router CCA tan solo 1.

El resto de valores sirven para el control de mensajes de control que han sido enviados y recibidos por parte del resto de vecinos. En la captura de pantalla se puede apreciar que desde que la sesión BGP llego al estado de Established, el router GYE aprendió todas sus rutas a través del enlace que conduce a R4-ISP1 con lo que se puede deducir que hubo un problema de conexión con el peer 20.2.2.2.

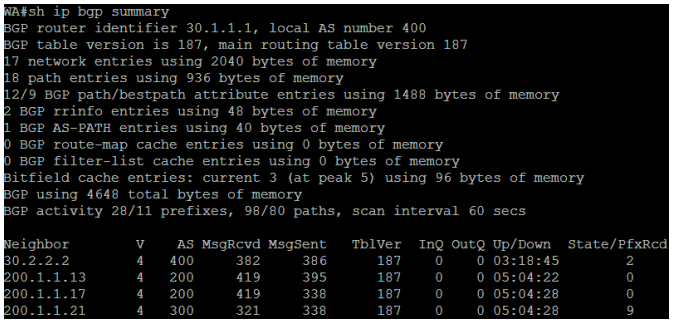


Figura 55 Tabla BGP-WA.

Realizado por: *Morales, W. 2016.*

El router WA con ID: 30.1.1.1 tiene un número interno de versión de la tabla de 187, se puede observar que ha aprendido 2 prefijos del peer 30.2.2.2 que se encuentra con una sesión iBGP establecida dentro del mismo AS400. Se puede ver la relación de vecindad que mantiene WA con peers como:

- *FL*
- *ISP 2*
- *Conexión Multi-homing hacia el ISP 1 con dos enlaces activos al AS200.*

En este caso el router WA ha aprendido todas las rutas eBGP por R4-ISP2, esto significa que en el momento de la captura de pantalla hubo una caída de conexión con el neighbor 20.3.3.3.

5.2.4.5. Peer-Groups

Para tener un mejor control de vecindades, así como hacer fácil las tareas de administración y mantenimiento de la red se optó por aplicar Peer-groups en ambos ASes Públicos; se estableció una plantilla para aplicarlas a todos los peers iBGP con el fin de compartir la misma información. Una buena práctica a realizarse y más aún si deseamos que la red sea escalable en el futuro, es optar por este mecanismo incluso si tenemos pocos peers iBGP. También existe la posibilidad de usar peer-groups en sesiones eBGP, especialmente si tenemos configuraciones como Puntos de Intercambio; un caso claro en nuestro país la AEPROVI la cual ata a la mayoría de ISPs de acceso de clientes para que el tráfico conmute más rápidamente a través de él, haciendo que el tráfico generado localmente no consuma ancho de banda utilizando enlaces internacionales.

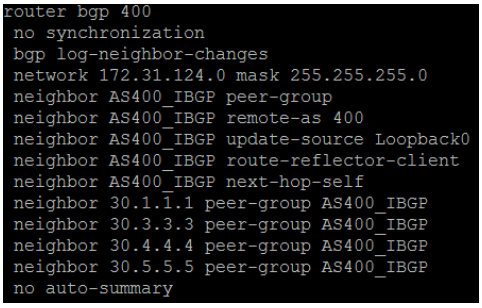


Figura 56 Configuración BGP.

Realizado por: *Morales, W. 2016.*

El concepto es el de tener un Switch de core que sirve de puente con los routers de borde de los ISPs del país, es una práctica muy aceptada en diversas partes de mundo para evitar varios problemas:

- *Evitar que un AS atado a un IPS del punto de intercambio se convierta en Tránsito*
- *Tener mayor control de las funciones de Damping*
- *Evitar publicar rutas que no han sido concesionadas*
- *No publicar los prefijos que están marcados con un Community*

Para hacer que realmente BGP tenga sentido es necesario usar técnicas del toolkit, varias de ellas aportan para que este protocolo sea robusto para redes escalables; las técnicas usadas son:

- *Route Refresh*
- *Peer groups*
- *Route flap damping*
- *Route Reflectors*
- *Confederaciones (antiguo)*

```
router bgp 100
 no synchronization
 bgp log-neighbor-changes
 network 128.10.110.0 mask 255.255.255.224
 network 128.10.110.32 mask 255.255.255.224
 neighbor AS100_IBGP peer-group
 neighbor AS100_IBGP remote-as 100
 neighbor AS100_IBGP update-source Loopback0
 neighbor AS100_IBGP route-reflector-client
 neighbor 10.1.1.1 peer-group AS100_IBGP
 neighbor 10.1.1.5 peer-group AS100_IBGP
 neighbor 10.1.1.9 peer-group AS100_IBGP
 neighbor 10.1.1.13 peer-group AS100_IBGP
 neighbor 10.1.1.21 peer-group AS100_IBGP
 no auto-summary
```

Figura 57 Configuración BGP.

Realizado por: *Morales, W. 2016.*

El problema al interior de un AS en peers iBGP puede resultar muy grave cuando se tiene un full mesh de sesiones entre muchos equipos, esto conlleva a una convergencia más lenta que lo normal. Las ventajas de usar Peer-groups son:

- *Configuración sencilla en redes escalables*
- *Hace que las configuraciones sean menos susceptibles a errores*
- *Procesamiento de CPU bajo*
- *El full mesh de sesiones iBGP se consolida más rápido*
- *Los miembros del grupo pueden tener varias políticas de enrutamiento*
- *Puede ser usado en sesiones eBGP*

5.2.4.6. Dampening

Se ha establecido la funcionalidad de damping sobre el ISP1 con el objetivo de simular las funciones que tienen los Tier 1 para evitar fluctuaciones de prefijos de red en el Internet. Esta función sirve para corregir las propagaciones de inestabilidad de una red cuando se recibe publicaciones que hacen flapping. Cuando un peer publica una red varias veces demostrando así que es inestable se penaliza cuando sobrepasa un umbral determinado; una vez penalizado se dará un tiempo exponencial determinado para volver aprender de ese peer.

Cada vez que se genera un damping se produce una onda de inestabilidad global en Internet, esto conlleva a que se re-calculen los paths y por ende a perder las rutas por

tiempos largos (dependiendo del ISP). Existe la posibilidad que las sesiones eBGP se mantengan up y se produzca flapeo en las rutas. El damping tiene la función de publicar rutas estables a internet, además de suprimir la oscilación de rutas.

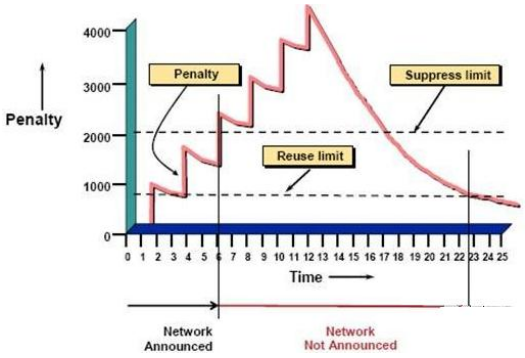


Figura 58 Dampening-BGP.

Fuente: *http://xuanbo.blog.51cto.com/499334/465596/*

Funcionamiento

En el siguiente ejemplo se puede explicar lo que pasaría si GYE flappea una ruta hacia R2-ISP1:

Suponiendo que a los 2 minutos después de haberse dado el peering entre los dos routers flapea la ruta 192.168.1.0; en ese momento se penaliza la ruta con 1000 puntos. En ese instante se tendrá un tiempo en el cual seguirá bajando exponencialmente la penalización, si a los 4 minutos de nuevo flapea la ruta se penalizará de nuevo. Si los puntos de penalizaciones sobrepasan el límite de supresión entonces la ruta dejará de ser aprendida por R2-ISP1 hasta que baje la penalización con una tasa de decaimiento establecida por el ISP hasta que se encuentre por debajo del límite de reuso. Después de dicho límite se considera que el prefijo se encuentra estable y nuevamente es aprendido por R2-ISP1.

La función de dampening solamente es aplicable en peers eBGP en anuncios de inbound, los valores por defecto son:

- *Velocidad de decaimiento: 15 minutos*
- *Límite de reuso: 750*

- *Límite de supresión: 2000*
- *Tiempo de supresión máxima: 1 hora*

*En un ambiente real se debe tener mucho cuidado con el comando **clear** al momento de hacer un Hard o Soft-Reconfiguration de las sesiones BGP, pues esto tira las sesiones con el peer eBGP y hace que las rutas se penalicen en el ISP, cayendo en damping y por ende quedando por fuera de la vista del mundo de Internet por varios minutos, incluso hasta 1 hora. Si se llegara a este punto, los usuarios del AS100 conocerían como llegar hacia el mundo de Internet, pero del otro lado no conocerán como llegar al AS. La implementación es relativamente fácil, pero hay que estar consciente del impacto que una mala configuración traería a la red ya que la mayoría de Los ISPs castigan severamente el damping.*

```
router bgp 200
 no synchronization
 bgp log-neighbor-changes
 bgp dampening route-map crio
 neighbor 20.1.1.1 remote-as 200
 neighbor 20.1.1.1 update-source Loopback0
 neighbor 20.1.1.1 next-hop-self
 neighbor 200.1.1.5 remote-as 100
 neighbor 200.1.1.9 remote-as 100
 no auto-summary
!
ip local policy route-map SSH
ip forward-protocol nd
!
!
ip http server
no ip http secure-server
!
ip access-list extended SSH
 permit tcp any any eq 22
 permit tcp any eq 22 any
!
!
ip prefix-list toto seq 5 permit 128.10.106.0/24 le 32
ip prefix-list toto seq 10 permit 128.10.107.0/24 le 32
ip prefix-list toto seq 15 permit 128.10.110.0/27 le 32
ip prefix-list toto seq 20 permit 128.10.110.32/27 le 32
ip prefix-list toto seq 25 permit 128.10.109.0/25 le 32
ip prefix-list toto seq 30 permit 128.10.109.128/25 le 32
ip prefix-list toto seq 35 permit 128.10.96.0/22 le 32
ip prefix-list toto seq 40 permit 128.10.100.0/22 le 32
ip prefix-list toto seq 45 permit 128.10.104.0/24 le 32
ip prefix-list toto seq 50 permit 128.10.105.0/24 le 32
ip prefix-list toto seq 55 permit 128.10.108.0/25 le 32
ip prefix-list toto seq 60 permit 128.10.108.128/25 le 32
access-list 25 deny   20.2.2.0
access-list 25 permit any
!
route-map crio permit 10
 match ip address prefix-list toto
 set dampening 30 2000 3000 60
!
```

Figura 59 Políticas de enrutamiento-R2_ISP1.

***Realizado por:** Morales, W. 2016.*

R2-ISP1 tiene configurado la función de dampening mediante un Route-map con el objetivo de especificar que redes se desea aplicar esta función, en este ejemplo todas las subredes del

AS100 pasaran a ser filtradas por el router de borde del ISP, y en caso de haber flapeo repetitivo de cualquiera de las subredes produzca que el valor de la penalización sea mayor que el límite de supresión hará que se genere un damping de 60 min para que la ruta quede por fuera de Internet.

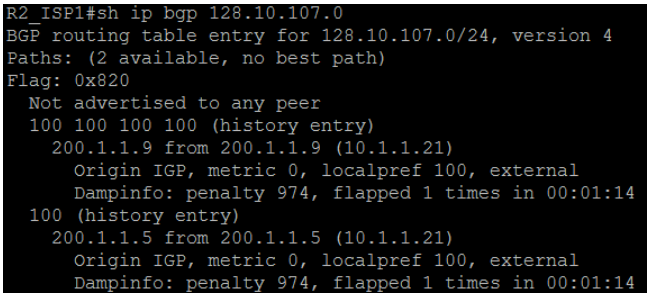


Figura 60 Penalidad BGP-R2_ISP1.

Realizado por: *Morales, W. 2016.*

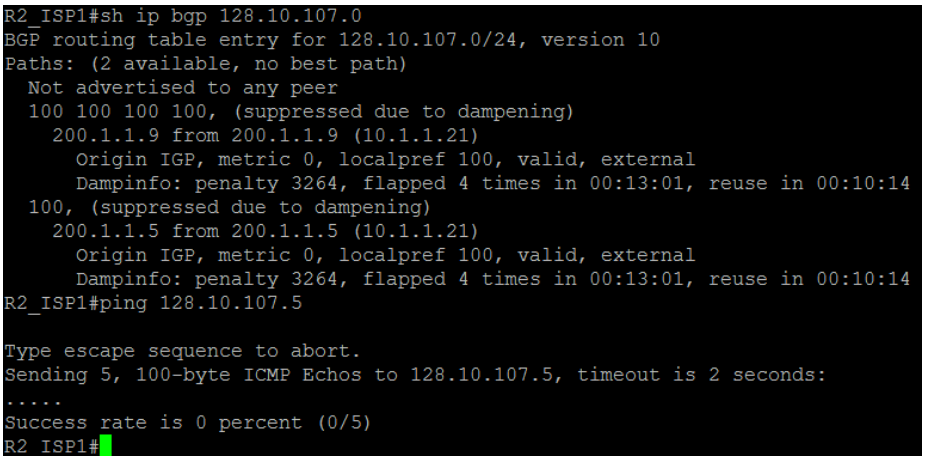


Figura 61 Demostración Dampening-R2_ISP1.

Realizado por: *Morales, W. 2016.*

Se puede observar que la subred 128.10.107.0 al flapear la primera vez tiene como penalidad 1000 puntos, enseguida la velocidad de decaimiento hace que baje exponencialmente hasta 974 puntos; al cuarto flapeo se observa que la penalidad es de 3264 puntos y la ruta queda por fuera hasta que la ruta baje del límite de reúso (2000 puntos).

5.2.4.7. Aggregation

La sumarización de rutas en BGP significa publicar un bloque de direcciones que nos ha proporcionado un RIR a otro AS conectado a nuestra red. La ventaja de este tipo de configuraciones en conexiones hacia un ISP es que los AS que implementan esta solución

colaborar indirectamente a que no existan olas de publicación de redes en Internet; si por ejemplo la subred 128.10.106.0/24 del router GYE cae por cualquier eventualidad, si no se tuviera configurado Aggregation en GYE haría que el router de borde del AS100 deje de anunciar esa ruta al exterior, por lo que el ISP1 podría tomar acciones como dampening hacia el AS100 con el fin de no producir inestabilidad en la red hacía por ejemplo su Tier1.

El tener una ruta "clavada" apuntando a Null, garantiza que la ruta siempre estará en GYE incluso si la red 128.10.106.0 cae. De esta forma GYE siempre publicará una ruta sumarizada al ISP1.

En muchos textos de referencia se hace énfasis en que los subprefijos de bloques de direcciones no deberían ser publicados a Internet a menos que hayan circunstancias especiales, esto se refiere a Multi-homing donde si es necesario enviar prefijos específicos. También es recomendable hacer Aggregation en los borders del AS, no en el interior de la topología ya que el border es el equipo que tiene conexión directa contra Internet.

En la figura se puede observar que se pone un filtro en sentido OUT, con el objetivo de permitir la red 128.10.106.0/24 y se niegue el resto de tráfico. Es recomendable usar filtros de este tipo para garantizar que no se publique redes que no le corresponden recibir al ISP; con eso se protege el Proveedor de Servicios que el AS100 se convierta en un AS de Tránsito.

En la medida de posible se recomienda no sumarizar en prefijos mayores a /24, si se puede sumarizar usando el prefijo que dio el RIR sería lo aconsejable.

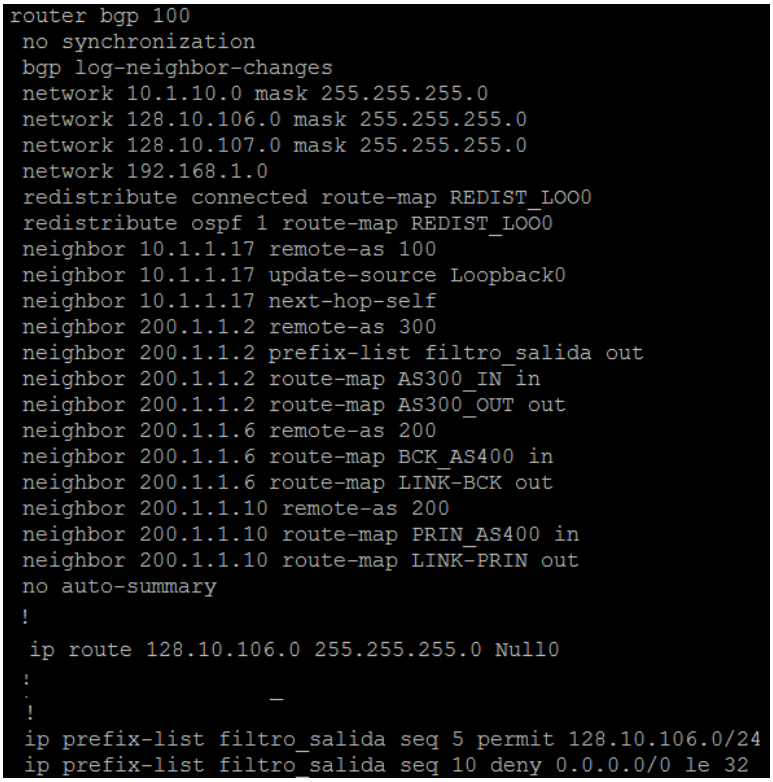


Figura 62 Configuración BGP-GYE.

Realizado por: *Morales, W. 2016.*

Otra desventaja de no usar Aggregation en el AS100 es que el router GYE puede percibir este comportamiento como una baja calidad de servicio QoS, ya que si flapea la ruta; la sesión eBGP todavía sigue estando activa y a pesar no de tener problemas de enrutamiento no se levanta en tráfico después del flapeo. Esto sucede porque se podría demorar varios minutos en llegar las actualizaciones BGP a los routers de borde del AS y as su vez esperar a que se actualicen las rutas que están en Internet por la fluctuación de enrutamiento.

Las ventajas de usar Aggregation:

- *Ayuda a que no existan olas de enrutamiento en Internet*
- *Reducen el tamaño de tablas RIB*
- *Mejora el QoS de Internet*
- *Impide penalizaciones por dampening*

Se debe tener en consideración los siguientes conceptos

- *Tier 1.- Son redes tipo privadas que permiten el intercambio de tráfico cruzando los respectivos backbones entre ISPs del mismo tipo, sin mantener alguna relación de costos. Tienen alcance internacional formando peerings entre los demás ISPs del mismo nivel, así como con algunos ISP de nivel 2.*
- *Tier 2.- Son redes que permiten la interconexión regional mediante el peering con otras redes del mismo tipo (generalmente con costo), así como con algunas redes de nivel 1. Son particularmente clientes Tier 1.*
- *Tier 3.- Son ISP de nivel jerárquico más bajos los cuales dan acceso a internet a usuarios finales. Los ISP de este tipo pueden formar peerings usando Puntos de Intercambio, similar al que se tiene en Ecuador (AEPROVI).*

5.2.4.8. Redistribución de rutas

La redistribución de rutas es un proceso que hay que tomarlo con las precauciones del caso ya que se debe hacer una planificación sobre el tipo de protocolo que se pretenda introducir en la topología de red; por ejemplo no podrían convivir dentro del mismo AS un protocolo como RIPV1 junto con protocolos de enrutamiento dinámico avanzado como lo EIGRP, OSPF y IS-IS. Es una buena opción utilizar el proceso de distribución cuando se trate de migrar redes a una sola; lo ideal sería manejar un solo protocolo de enrutamiento en un sistema autónomo, y por cuestiones de seguridad, redundancia utilizar otro protocolo de enrutamiento y realizar la distribución de la información de enrutamiento con las medidas del caso. Es de consideración al momento de implementar la distribución conocer que no se pueden mezclar procesos que manejan distintos tipos de direccionamiento IP (IPv4-IPv6).

```
router eigrp 100
 redistribute ospf 1 metric 64 100 255 1 1500
 network 128.10.0.0
 auto-summary
router ospf 1
 log-adjacency-changes
 area 100 nssa
 area 200 virtual-link 10.1.1.17
 area 200 virtual-link 192.168.2.1
 redistribute connected subnets
 redistribute eigrp 100 subnets
 network 10.1.1.12 0.0.0.3 area 100
 network 10.1.0.0 0.0.255.255 area 100
 network 128.10.104.0 0.0.0.255 area 100
 network 128.10.105.0 0.0.0.255 area 100
 network 128.10.110.76 0.0.0.3 area 100
router bgp 100
 no synchronization
 bgp log-neighbor-changes
 network 10.1.10.0 mask 255.255.255.0
 network 128.10.106.0 mask 255.255.255.0
 network 128.10.107.0 mask 255.255.255.0
 network 192.168.1.0
 redistribute connected route-map REDIST_LOO0
 redistribute ospf 1 route-map REDIST_LOO0
```

Figura 63 Redistribución de rutas.

Realizado por: *Morales, W. 2016.*

Antes de comenzar con la redistribución de rutas es importante tener en cuenta que no todos los protocolos de enrutamiento manejan similares formas para encontrar los mejores caminos hacia los destinos, por ejemplo RIP usa una métrica basada en saltos ni mayores a 16. EIGRP tiene una métrica compuesta de diversos elementos como el Ancho de banda, confiabilidad, carga, retardo y MTU. Por otro lado OSPF escoge los mejores paths por medio del Ancho de banda. IS-IS por su lado maneja cuatro tipos de métricas siendo la que maneja por defecto Cisco con un coste de 10, para escoger el mejor camino hacia un destino se escoge la métrica más baja,mientras que las rutas externas son preferidas sobre las internas al igual que los routers de Nivel 1 tienen preferencia sobre routers de Nivel 2. Es por esta razón que cuando intercambian información de enrutamiento entre protocolos de capa 3 hay una incompatibilidad entre métricas. Es necesario buscar la forma de manejar una base para calcular la métrica, este nuevo coste es llamado "Semilla" acompañado de la Distancia Administrativa.

Esta semilla o métrica base es la siguiente:

- *EIGRP (Costo Infinito)*
- *OSPF (Costo de 20 para rutas O E2, costo de 1 para rutas O E1)*
- *IS-IS (0)*
- *BGP (Multi-Exit Discriminator: Usado para influir sobre los neighbors el tráfico de Upstram)*

Pueden existir múltiples problemas cuando se necesite redistribuir, entre los problemas más comunes está la creación de loops de enrutamiento donde un paquete puede quedarse dando vueltas dentro del AS de forma indefinida. También puede resultar en que se escoja de manera equívoca los mejores caminos hacia los destinos; así como tiempos lentos para converger las tablas de enrutamiento.

Para comprobar que toda la topología tiene conectividad total, se puede observar las tablas de enrutamiento de cada equipo donde se puede observar que todas las redes son alcanzables. Además se ha optado por comprobar la alcanzabilidad de los prefijos de Loopback en cada caso cruzando todos los Sistemas Autónomos para demostrar que efectivamente la redistribución de rutas y la convergencia de todos los protocolos de enrutamiento están funcionando correctamente.

Esta prueba se realiza desde el router TX localizado en el Sistema Autónomo 400 hasta todas las redes remotas del Sistema Autónomo 100.

5.2.4.9. PRUEBAS DE CONECTIVIDAD

```
TX#ping 10.1.1.1 source loopback 0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.5, timeout is 2 seconds:
Packet sent with a source address of 30.3.3.3
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 112/113/116 ms
```

Figura 64 Ping-TX, UIO.

Realizado por: *Morales, W. 2016.*

```
TX#ping 10.1.1.13 source loopback 0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.13, timeout is 2 seconds:
Packet sent with a source address of 30.3.3.3
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 112/151/300 ms
```

Figura 65 Ping-TX, IMB.

Realizado por: *Morales, W. 2016.*

```
TX#ping 10.1.1.9 source loopback 0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.9, timeout is 2 seconds:
Packet sent with a source address of 30.3.3.3
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 112/142/264 ms
```

Figura 66 Ping-TX, LJA.

Realizado por: *Morales, W. 2016.*

```
TX#ping 10.1.1.5 source loopback 0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.5, timeout is 2 seconds:
Packet sent with a source address of 30.3.3.3
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 112/114/116 ms
```

Figura 67 Ping-TX, AMB.

Realizado por: *Morales, W. 2016.*

```
TX#ping 10.1.1.17 source loopback 0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.17, timeout is 2 seconds:
Packet sent with a source address of 30.3.3.3
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/60/72 ms
```

Figura 68 Ping-TX, CCA.

Realizado por: *Morales, W. 2016.*

```
TX#ping 10.1.1.21 source loopback 0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.21, timeout is 2 seconds:
Packet sent with a source address of 30.3.3.3
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/65/100 ms
```

Figura 69 Ping-TX, GYE.

Realizado por: *Morales, W. 2016.*

```
TX#ping 30.1.1.1 source loopback 0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 30.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 30.3.3.3
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/30/32 ms
```

Figura 70 Ping-TX, WA.

Realizado por: *Morales, W. 2016.*

```
TX#ping 30.2.2.2 source loopback 0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 30.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 30.3.3.3
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/29/32 ms
```

Figura 71 Ping-TX, FL.

Realizado por: *Morales, W. 2016.*

```
TX#ping 30.4.4.4 source loopback 0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 30.4.4.4, timeout is 2 seconds:
Packet sent with a source address of 30.3.3.3
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/32 ms
```

Figura 72 Ping-TX, NY.

Realizado por: *Morales, W. 2016.*

```
TX#ping 30.5.5.5 source loopback 0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 30.5.5.5, timeout is 2 seconds:
Packet sent with a source address of 30.3.3.3
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/29/32 ms
```

Figura 73 Ping-TX, CA.

Realizado por: *Morales, W. 2016.*

```
TX#ping 192.168.1.7 source loopback 0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.7, timeout is 2 seconds:
Packet sent with a source address of 30.3.3.3
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/96/216 ms
```

Figura 74 Ping-TX, CACTI.

Realizado por: *Morales, W. 2016.*

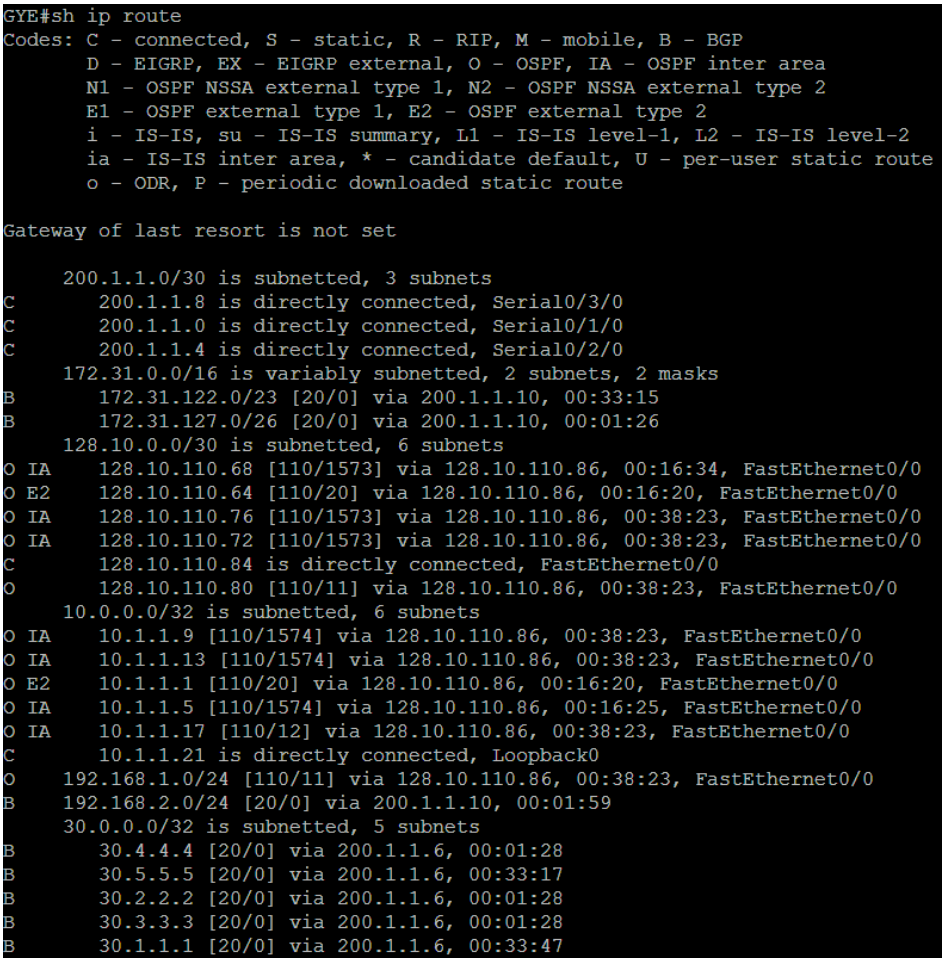


Figura 75 Tabla de enrutamiento-GYE.

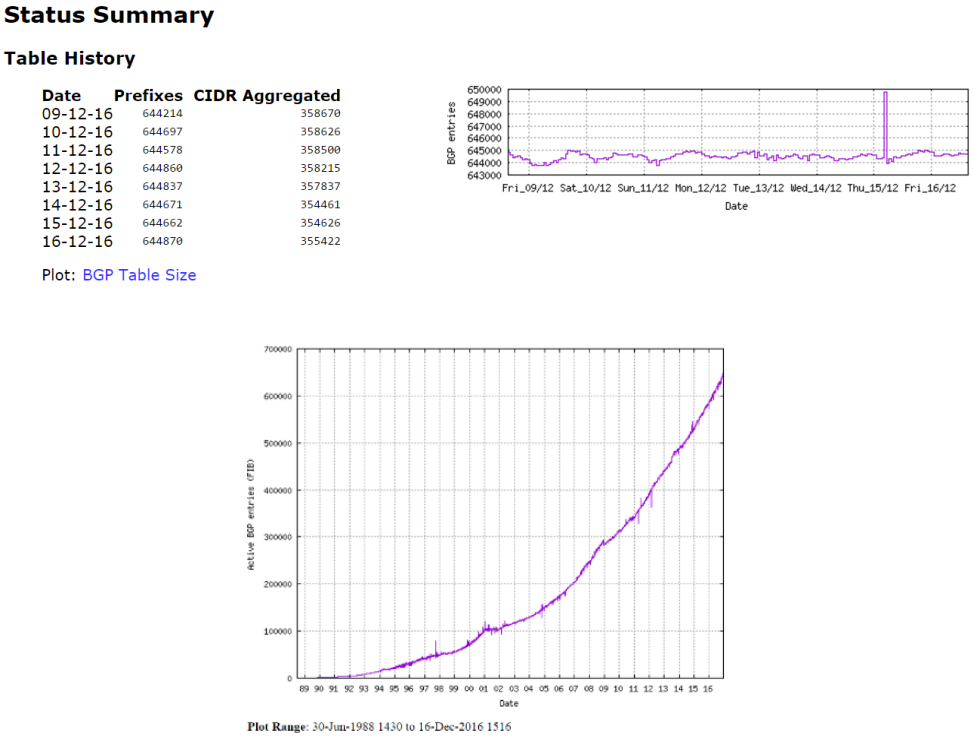
Realizado por: *Morales, W. 2016.*

6. Implementar una topología redundante a nivel de LAN con el uso del protocolo GLBP, a nivel de WAN mediante el toolkit de BGP y Multi-Homing, así como a nivel de Firewall mediante enlaces redundantes y tracking de objetos para tener alta disponibilidad.

6.1. Politicas de enrutamiento BGP-AS100

BGP es uno de los protocolos más robustos que existen actualmente y precisamente es el único que puede manejar todas las tablas de enrutamiento que existe en Internet la cual bordea las 645000 rutas. Es por esta razón que los prefijos de clientes no deben mezclarse en el IGP de un sistema autónomo, los protocolos de enrutamiento internos le sirven a BGP para tener estabilidad en la topología y para llevar información de enrutamiento interno del AS. Por otro lado ningún protocolo IGP puede manipular tráfico de upstream como downstream como lo

hace BGP; y esa característica hace de este protocolo que sea ideal para trabajar uniendo redes y sistemas autónomos que llevan mucha información de enrutamiento.



Status Summary

Table History

Date	Prefixes	CIDR Aggregated
09-12-16	644214	358670
10-12-16	644697	358626
11-12-16	644578	358500
12-12-16	644860	358215
13-12-16	644837	357837
14-12-16	644671	354461
15-12-16	644662	354626
16-12-16	644870	355422

Plot: BGP Table Size

Plot Range: 30-Jun-1988 1430 to 16-Dec-2016 1516

Figura 76 Crecimiento de rutas BGP.

Fuente: *http://cidr-report.org/*

En el presente caso de estudio se han implementado las siguientes políticas de enrutamiento para el AS100:

- *Todo el tráfico de upstream generado desde el AS 100 destinado a las interfaces fastethernet 0/0 del AS400, serán llevadas a través del enlace serial 200.1.1.8/30 considerado como "Principal" que conecta con el ISP1.*
- *Todo el tráfico de upstream generado desde el AS 100 destinado a las interfaces fastethernet 0/1 del AS400, serán llevadas a través del enlace serial 200.1.1.4/30 considerado como "Backup" que conecta con el ISP1.*
- *En caso que la sesión eBGP hacia el peer 20.2.2.2 establecida por el enlace Principal caiga, todo el tráfico de upstream debe pasar a la interfaz de Backup.*
- *En caso que la sesión eBGP hacia el peer 20.2.2.2 establecida por el enlace de Backup caiga, todo el tráfico de upstream debe pasar a la interfaz que conecta al ISP2.*

- *En caso de restablecimiento de enlaces, el tráfico debe volver a circular como las políticas lo plantean.*

Como se observa en la configuración de BGP existen 4 etapas de configuración:

- *La primera etapa es levantar el IGP de todo el Sistema Autónomo 100, usando los protocolos de enrutamiento dinámico descritos anteriormente con la ayuda de redistribución de rutas. Esto con el objetivo que todas las rutas se conozcan al interior de AS para dejar todo el camino libre y estable para que entre a funcionar BGP.*
- *La segunda etapa está concentrada en establecer un full mesh de sesiones iBGP usando como interfaz de control las direcciones de Loopback con una máscara /32 para que no dependa del IGP ni a interfaces físicas. Adicional a esto, se implementa un mecanismo para que la topología sea escalable con el tiempo, esto es con la configuración de un esquema de Route-Reflector, donde todos los routers clientes formarán adyacencias con el R-R CCA.*
- *La tercera etapa consiste en levantar las respectivas sesiones eBGP entre el AS100, AS200, AS300 cambiando el Next-Hop a las interfaces de Loopback, ya que al ser interfaces virtuales nunca caerán a menos que administrativamente se lo haga o el router falle.*
- *La cuarta etapa es configurar las políticas de enrutamiento usando las capabilities de BGP en conjunto con el toolkit que ofrece el protocolo tales como: Prefix-lists, y Route-maps.*
- *La quinta y última etapa está pensada en cuidar que el AS100 no se convierta en AS de Tránsito y cuidarse de penalizaciones por dampening.*

```
router bgp 100
 no synchronization
 bgp log-neighbor-changes
 network 10.1.10.0 mask 255.255.255.0
 network 128.10.106.0 mask 255.255.255.0
 network 128.10.107.0 mask 255.255.255.0
 network 192.168.1.0
 redistribute connected route-map REDIST_LOO0
 redistribute ospf 1 route-map REDIST_LOO0
 neighbor 10.1.1.17 remote-as 100
 neighbor 10.1.1.17 update-source Loopback0
 neighbor 10.1.1.17 next-hop-self
 neighbor 200.1.1.2 remote-as 300
 neighbor 200.1.1.2 route-map AS300_IN in
 neighbor 200.1.1.2 route-map AS300_OUT out
 neighbor 200.1.1.6 remote-as 200
 neighbor 200.1.1.6 route-map BCK_AS400 in
 neighbor 200.1.1.6 route-map LINK-BCK out
 neighbor 200.1.1.10 remote-as 200
 neighbor 200.1.1.10 route-map PRIN_AS400 in
 neighbor 200.1.1.10 route-map LINK-PRIN out
 no auto-summary
```

Figura 77 Configuración BGP-GYE.

Realizado por: *Morales, W. 2016.*

Como se observa en la figura, el router de frontera utiliza el comando network para publicar a sus vecinos las redes que tiene conectadas directamente y que como requisito para que sus peers vean estas rutas es que se encuentren en la tabla RIB.

Adicionalmente se hace la redistribución de rutas que se encuentran atadas al equipo, además de publicar todas las redes OSPF del AS.

Por último se utilizan Route-maps para realizar las políticas de enrutamiento tanto en el sentido entrante como saliente del router GYE.

```
ip prefix-list BCK seq 5 permit 128.10.108.128/25
ip prefix-list BCK seq 10 permit 128.10.105.0/24
ip prefix-list BCK seq 15 permit 128.10.100.0/22
ip prefix-list BCK seq 20 permit 128.10.109.128/25
ip prefix-list BCK seq 25 permit 128.10.110.32/27
ip prefix-list BCK seq 30 permit 128.10.107.0/24
!
ip prefix-list BCK_AS100 seq 5 permit 128.10.108.128/25
ip prefix-list BCK_AS100 seq 10 permit 128.10.105.0/24
ip prefix-list BCK_AS100 seq 15 permit 128.10.100.0/22
ip prefix-list BCK_AS100 seq 20 permit 128.10.109.128/25
ip prefix-list BCK_AS100 seq 25 permit 128.10.110.32/27
ip prefix-list BCK_AS100 seq 30 permit 128.10.107.0/24
!
ip prefix-list BCK_AS400 seq 5 permit 172.31.127.64/26
!
ip prefix-list LOO0_AS100 seq 5 permit 10.0.0.0/8 ge 32
!
ip prefix-list LOO0_AS400 seq 5 permit 30.0.0.0/8 ge 32
```

Figura 78 Prefix-list-GYE.

Realizado por: *Morales, W. 2016.*

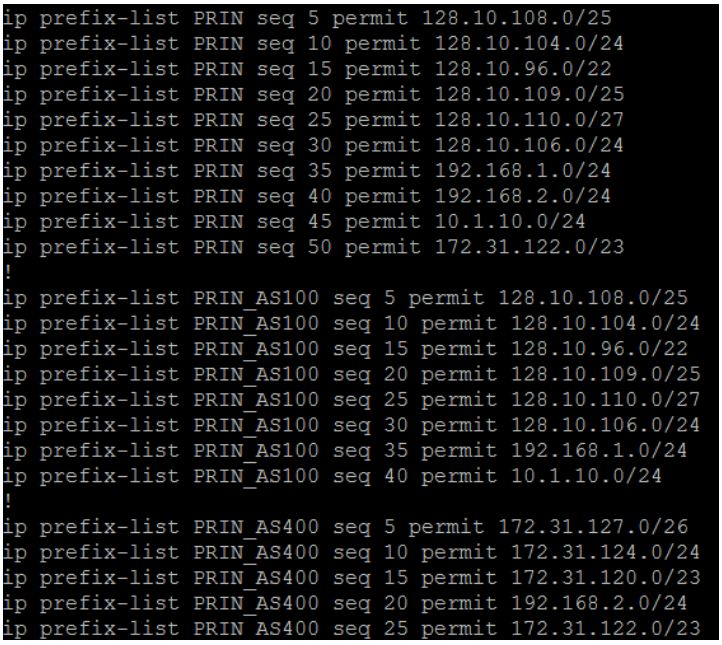


Figura 79 Políticas de manipulación de tráfico-GYE

Realizado por: *Morales, W. 2016.*

En estos Prefix-lists se establecen que subredes pasarán por el enlace Principal y cual por el enlace de Backup. Por ejemplo:

- *La subred 172.31.127.0/26 que se encuentra en la interfaz Fastethernet 0/0 del router NY deberá circular por el enlace Principal hacia el ISP2 usando el Prefix-List PRIN_400.*
- *La subred 172.31.127.64/26 que se encuentra en la interfaz Fastethernet 0/1 del router NY deberá circular por el enlace Secundario hacia el ISP2 usando el Prefix-List BCK_AS400.*

Mediante el atributo AS_PATH y Local Preference se influye para tener el control y manipulación del tráfico por ciertas interfaces como en el presente caso.

```
route-map LINK-PRIN permit 10
 match ip address prefix-list PRIN_AS100
!
route-map LINK-PRIN permit 20
 match ip address prefix-list BCK_AS100 LOO0_AS100
 set as-path prepend 100 100 100
!
route-map AS300_OUT permit 10
 match ip address prefix-list LOO0_AS100 PRIN_AS100 BCK_AS100
 set as-path prepend 100 100 100 100 100
!
route-map BCK_AS400 permit 10
 match ip address prefix-list BCK_AS400 LOO0_AS400
!
route-map BCK_AS400 permit 20
 match ip address prefix-list PRIN_AS400
 set local-preference 90
!
route-map REDIST_LOO0 permit 10
 match ip address prefix-list LOO0_AS100
!
route-map SSH permit 10
 match ip address SSH
 set interface Serial0/3/0
!
route-map SSH permit 20
!
route-map LINK-BCK permit 10
 match ip address prefix-list BCK_AS100 LOO0_AS100
!
route-map LINK-BCK permit 20
 match ip address prefix-list PRIN_AS100
 set as-path prepend 100 100 100
!
route-map LINK-BCK permit 100
!
route-map AS300_IN permit 10
 set local-preference 50
!
route-map PRIN_AS400 permit 10
 match ip address prefix-list PRIN_AS400
!
route-map PRIN_AS400 permit 20
 match ip address prefix-list BCK_AS400 LOO0_AS400
 set local-preference 90
```

Figura 80 Manipulación de tráfico.

Realizado por: *Morales, W. 2016.*

6.2. Politicas de enrutamiento BGP-AS400

En el presente caso de estudio se han implementado las siguientes políticas de enrutamiento para el AS400:

- *Todo el tráfico de upstream generado desde el AS 400 destinado a las interfaces fastethernet 0/0 del AS100, serán llevadas a través del enlace serial 200.1.1.16/30 considerado como "Principal" que conecta con el ISP1.*
- *Todo el tráfico de upstream generado desde el AS 400 destinado a las interfaces fastethernet 0/1 del AS100, serán llevadas a través del enlace serial 200.1.1.12/30 considerado como "Backup" que conecta con el ISP1.*

- *En caso que la sesión eBGP hacia el peer 20.2.2.2 establecida por el enlace Principal caiga, todo el tráfico de upstream debe pasar a la interfaz de Backup.*
- *En caso que la sesión eBGP hacia el peer 20.2.2.2 establecida por el enlace de Backup caiga, todo el tráfico de upstream debe pasar a la interfaz que conecta al ISP2.*
- *En caso de restablecimiento de enlaces, el tráfico debe volver a circular como las políticas lo plantean.*

```
router bgp 400
 no synchronization
 bgp log-neighbor-changes
 network 172.31.122.0 mask 255.255.254.0
 network 192.168.2.0
 redistribute connected route-map REDIST_LOO0
 redistribute ospf 1 route-map REDIST_LOO0
 neighbor 30.2.2.2 remote-as 400
 neighbor 30.2.2.2 update-source Loopback0
 neighbor 30.2.2.2 next-hop-self
 neighbor 200.1.1.13 remote-as 200
 neighbor 200.1.1.13 route-map BCK_AS100 in
 neighbor 200.1.1.13 route-map BCK_AS400 out
 neighbor 200.1.1.17 remote-as 200
 neighbor 200.1.1.17 route-map PRIN_AS100 in
 neighbor 200.1.1.17 route-map PRIN_AS400 out
 neighbor 200.1.1.21 remote-as 300
 neighbor 200.1.1.21 route-map AS300_IN in
 neighbor 200.1.1.21 route-map AS300_OUT out
```

Figura 81 Configuración BGP-WA.

Realizado por: *Morales, W. 2016.*

```
ip prefix-list BCK_AS100 seq 5 permit 128.10.108.128/25
ip prefix-list BCK_AS100 seq 10 permit 128.10.105.0/24
ip prefix-list BCK_AS100 seq 15 permit 128.10.100.0/22
ip prefix-list BCK_AS100 seq 20 permit 128.10.109.128/25
ip prefix-list BCK_AS100 seq 25 permit 128.10.110.32/27
ip prefix-list BCK_AS100 seq 30 permit 128.10.107.0/24
!
ip prefix-list BCK_AS400 seq 5 permit 172.31.127.64/26
ip prefix-list BCK_AS400 seq 10 permit 172.31.122.0/23
!
ip prefix-list LOO0_AS100 seq 5 permit 10.0.0.0/8 ge 32
!
ip prefix-list LOO0_AS400 seq 5 permit 30.0.0.0/8 ge 32
!
ip prefix-list PRIN_AS100 seq 5 permit 128.10.108.0/25
ip prefix-list PRIN_AS100 seq 10 permit 128.10.104.0/24
ip prefix-list PRIN_AS100 seq 15 permit 128.10.96.0/22
ip prefix-list PRIN_AS100 seq 20 permit 128.10.109.0/25
ip prefix-list PRIN_AS100 seq 25 permit 128.10.110.0/27
ip prefix-list PRIN_AS100 seq 30 permit 128.10.106.0/24
ip prefix-list PRIN_AS100 seq 35 permit 192.168.1.0/24
ip prefix-list PRIN_AS100 seq 40 permit 10.1.10.0/24
!
ip prefix-list PRIN_AS400 seq 5 permit 172.31.127.0/26
ip prefix-list PRIN_AS400 seq 10 permit 172.31.124.0/24
ip prefix-list PRIN_AS400 seq 15 permit 172.31.120.0/23
ip prefix-list PRIN_AS400 seq 20 permit 192.168.2.0/24
ip prefix-list PRIN_AS400 seq 25 permit 172.31.122.0/24
```

Figura 82 Políticas BGP.WA.

Realizado por: *Morales, W. 2016.*

```
route-map AS300_OUT permit 10
 match ip address prefix-list PRIN_AS400 BCK_AS400 LOO0_AS400
 set as-path prepend 400 400 400 400 400
!
route-map BCK_AS400 permit 10
 match ip address BCK_AS400 LOO0_AS400
!
route-map BCK_AS400 permit 20
 match ip address PRIN_AS400
 set as-path prepend 400 400 400
!
route-map BCK_AS100 permit 10
 match ip address prefix-list BCK_AS100 LOO0_AS100
!
route-map BCK_AS100 permit 20
 match ip address prefix-list PRIN_AS100
 set local-preference 90
!
route-map REDIST_LOO0 permit 10
 match ip address prefix-list LOO0_AS400
!
route-map SSH permit 10
 match ip address SSH
 set interface Serial1/1
!
route-map SSH permit 20
!
route-map PRIN_AS100 permit 10
 match ip address prefix-list PRIN_AS100
!
route-map PRIN_AS100 permit 20
 match ip address prefix-list BCK_AS100 LOO0_AS100
 set local-preference 90
!
route-map AS300_IN permit 10
 set local-preference 50
!
route-map PRIN_AS400 permit 10
 match ip address prefix-list PRIN_AS400
!
route-map PRIN_AS400 permit 20
 match ip address prefix-list BCK_AS400 LOO0_AS400
 set as-path prepend 400 400 400
```

Figura 83 Políticas BGP.WA.

Realizado por: *Morales, W. 2016.*

6.3. Manipulación de tráfico - Protocolo de enrutamiento BGP

6.3.1.Sistema Atónomo 100 - Sistema Autónomo 400

Con el fin de hacer las respectivas pruebas de las políticas de enrutamiento de BGP, se procede a verificar la tabla de enrutamiento a una subred específica usando el comando ***show ip route [red de destino]*** *dando los siguientes resultados:*

- *Cuando GYE necesita alcanzar la subred 172.31.127.0/26 que corresponde a la interfaz fastethernet f0/0 del Router NY en el AS400, la ruta sugiere que el tráfico de upstream circule a través de la interfaz 200.1.1.8/32 considerada como Principal. En esta prueba realizada todos los enlaces se encuentran activos y en estado up.*

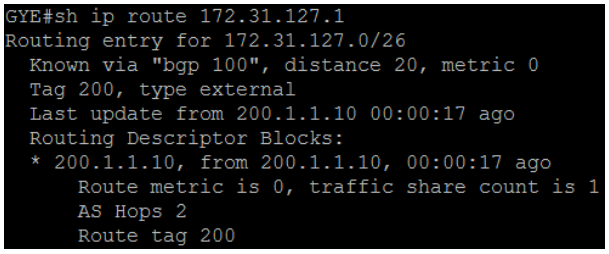


Figura 84 Ruta específica-GYE.

Realizado por: *Morales, W. 2016.*

- *Cuando GYE necesita alcanzar la subred 172.31.127.64/26 que corresponde a la interfaz fastethernet f0/1 del Router NY en el AS400, la ruta sugiere que el tráfico de upstream circule a través de la interfaz 200.1.1.4/32 considerada como Backup. En esta prueba realizada todos los enlaces se encuentran activos y en estado UP, excepto en enlace Principal a ISP1.*

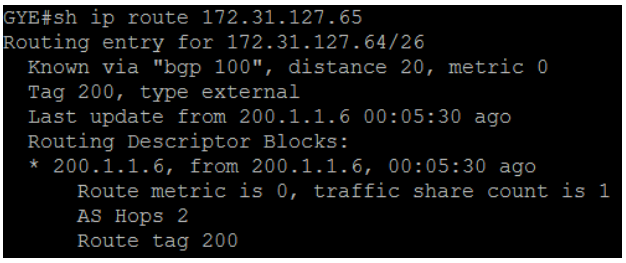


Figura 85 Ruta específica-GYE.

Realizado por: *Morales, W. 2016.*

- *Cuando GYE necesita alcanzar la subred 172.31.127.0/26 que corresponde a la interfaz fastethernet f0/0 del Router NY en el AS400, la ruta sugiere que el tráfico de upstream circule a través de la interfaz 200.1.1.2/32 considerada como Secundaria. En esta prueba realizada los dos enlaces (Principal, Backup) a ISP1 se encuentran en estado DOWN.*

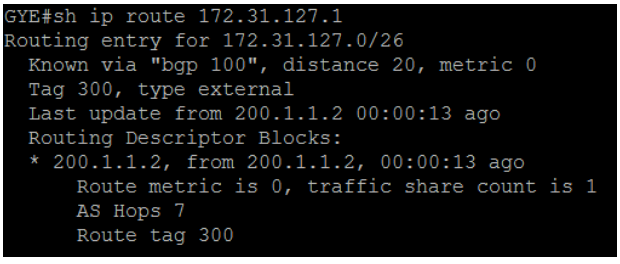


Figura 86 Ruta específica-GYE.

Realizado por: *Morales, W. 2016.*

Se procede a realizar pruebas de políticas de enrutamiento de BGP usando terminales, para lo cual se hace uso de los comandos ***ping [host]*** *y* ***tracert [destino]****.*

- *Se procede a verificar alcanzabilidad entre un host ubicado en la interfaz fastethernet 0/1 de IMB hacia el host localizado en la interfaz fastethernet 0/0 del router NY ubicado en el AS400; dando como resultado que el tráfico de upstream circule a través de la interfaz 200.1.1.8/32 considerada como Principal. En esta prueba realizada todos los enlaces se encuentran activos y en estado up.*

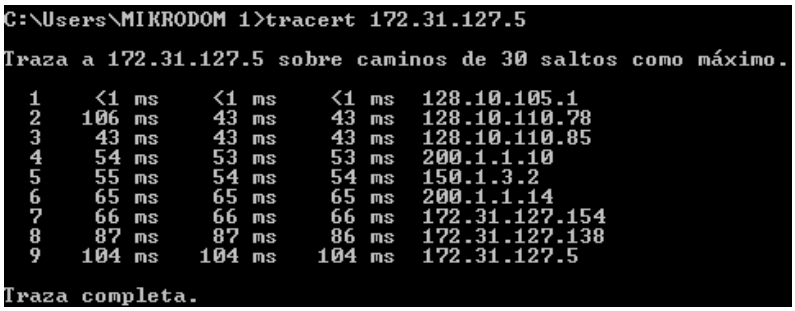


Figura 87 Pruebas BGP.

Realizado por: *Morales, W. 2016.*

- *Se procede a verificar alcanzabilidad entre un host ubicado en la interfaz fastethernet 0/1 de IMB hacia el host localizado en la interfaz fastethernet 0/0 del router NY ubicado en el AS400; dando como resultado que el tráfico de upstream circule a través de la interfaz 200.1.1.4/32 considerada como Secundaria. En esta prueba realizada todos los enlaces se encuentran activos y en estado UP, excepto en enlace Principal a ISP1.*

Figura 88 Pruebas BGP.

Realizado por: *Morales, W. 2016.*

- *Se procede a verificar alcanzabilidad entre un host ubicado en la interfaz fastethernet 0/1 de IMB hacia el host localizado en la interfaz fastethernet 0/0 del router NY ubicado*

en el AS400; dando como resultado que el tráfico de upstream circule a través de la interfaz 200.1.1.0/32 considerada como Secundaria. En esta prueba realizada los dos enlaces (Principal, Backup) a ISP1 se encuentran en estado DOWN.

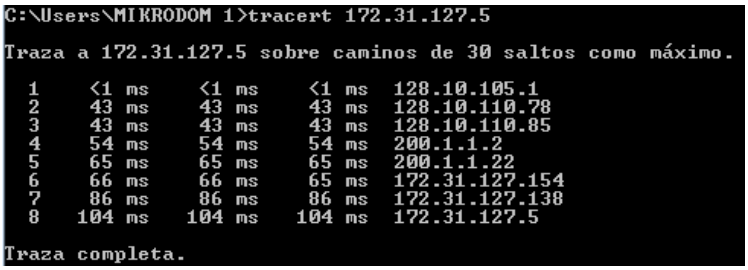


Figura 89 Pruebas BGP.

Realizado por: *Morales, W. 2016.*

- *Se procede a verificar alcanzabilidad entre un host ubicado en la interfaz fastethernet 0/1 de AMB hacia el host localizado en la interfaz fastethernet 0/1 del router NY ubicado en el AS400; dando como resultado que el tráfico de upstream circule a través de la interfaz 200.1.1.4/32 considerada como Backup. En esta prueba realizada todos los enlaces se encuentran activos y en estado up.*

Figura 90 Pruebas BGP.

Realizado por: *Morales, W. 2016.*

- *Se procede a verificar alcanzabilidad entre un host ubicado en la interfaz fastethernet 0/1 de AMB hacia el host localizado en la interfaz fastethernet 0/1 del router NY ubicado en el AS400; dando como resultado que el tráfico de upstream circule a través de la interfaz 200.1.1.8/32 considerada como Principal. En esta prueba realizada el enlace Backup se encuentra en estado DOWN.*

Figura 91 Pruebas BGP.

Realizado por: *Morales, W. 2016.*

- *Se procede a verificar alcanzabilidad entre un host ubicado en la interfaz fastethernet 0/1 de AMB hacia el host localizado en la interfaz fastethernet 0/1 del router NY ubicado en el AS400; dando como resultado que el tráfico de upstream circule a través de la interfaz 200.1.1.0/32 considerada como Secundario. En esta prueba realizada los dos enlaces (Principal, Backup) a ISP1 se encuentran en estado DOWN.*

Figura 92 Pruebas BGP.

Realizado por: *Morales, W. 2016.*

6.3.2. Sistema Atónomo 400 - Sistema Autónomo 100

- *Cuando WA necesita alcanzar la subred 128.10.109.0/25 que corresponde a la interfaz fastethernet f0/0 del Router AMB en el AS100, la ruta sugiere que el tráfico de upstream circule a través de la interfaz 200.1.1.17/32 considerada como Principal. En esta prueba realizada todos los enlaces se encuentran activos y en estado UP.*

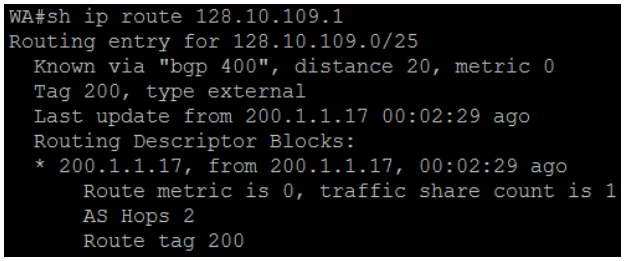


Figura 93 Ruta específica-WA.

Realizado por: *Morales, W. 2016.*

- *Cuando WA necesita alcanzar la subred 128.10.109.128/25 que corresponde a la interfaz fastethernet f0/1 del Router AMB en el AS100, la ruta sugiere que el tráfico de upstream circule a través de la interfaz 200.1.1.12/32 considerada como Backup. En esta prueba realizada todos los enlaces se encuentran activos y en estado UP, excepto en enlace Principal a ISP1.*

```
WA#sh ip route 128.10.109.129
Routing entry for 128.10.109.128/25
  Known via "bgp 400", distance 20, metric 0
  Tag 200, type external
  Last update from 200.1.1.13 00:03:24 ago
  Routing Descriptor Blocks:
  * 200.1.1.13, from 200.1.1.13, 00:03:24 ago
      Route metric is 0, traffic share count is 1
      AS Hops 2
      Route tag 200
```

Figura 94 Ruta específica-WA.

Realizado por: *Morales, W. 2016.*

- *Cuando WA necesita alcanzar la subred 128.10.109.128/25 que corresponde a la interfaz fastethernet f0/1 del Router AMB en el AS100, la ruta sugiere que el tráfico de upstream circule a través de la interfaz 200.1.1.20/32 considerada como Secundaria. En esta prueba realizada los dos enlaces (Principal, Backup) a ISP1 se encuentran en estado DOWN.*

```
WA#sh ip route 128.10.109.129
Routing entry for 128.10.109.128/25
  Known via "bgp 400", distance 20, metric 0
  Tag 300, type external
  Last update from 200.1.1.21 00:01:56 ago
  Routing Descriptor Blocks:
  * 200.1.1.21, from 200.1.1.21, 00:01:56 ago
      Route metric is 0, traffic share count is 1
      AS Hops 7
      Route tag 300
```

Figura 95 Ruta específica-WA.

Realizado por: *Morales, W. 2016.*

Se procede a realizar pruebas de políticas de enrutamiento de BGP usando terminales, para lo cual se hace uso de los comandos ***ping [host]*** *y* ***tracert [destino]****.*

- *Se procede a verificar alcanzabilidad entre un host ubicado en la interfaz fastethernet 0/1 de NY hacia el host localizado en la interfaz fastethernet 0/1 del router IMB ubicado en el AS100; dando como resultado que el tráfico de upstream circule a través de la*

interfaz 200.1.1.12/32 considerada como Principal. En esta prueba realizada el enlace Backup se encuentra en estado DOWN.

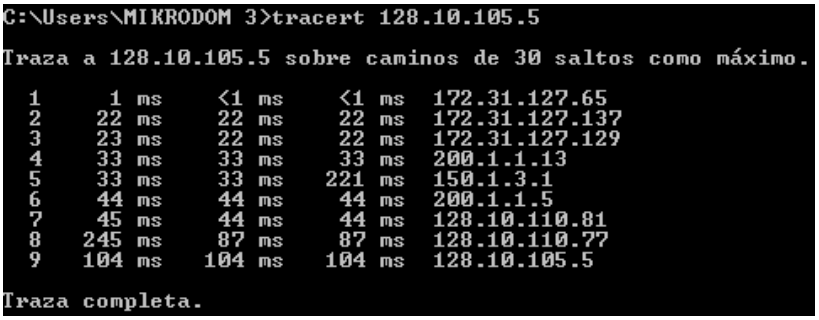


Figura 96 Pruebas BGP.

Realizado por: *Morales, W. 2016.*

- *Se procede a verificar alcanzabilidad entre un host ubicado en la interfaz fastethernet 0/1 de NY hacia el host localizado en la interfaz fastethernet 0/1 del router IMB ubicado en el AS100; dando como resultado que el tráfico de upstream circule a través de la interfaz 200.1.1.16/32 considerada como Principal. En esta prueba realizada el enlace Backup se encuentra en estado DOWN.*

Figura 97 Pruebas BGP.

Realizado por: *Morales, W. 2016.*

- *Se procede a verificar alcanzabilidad entre un host ubicado en la interfaz fastethernet 0/1 de NY hacia el host localizado en la interfaz fastethernet 0/1 del router IMB ubicado en el AS100; dando como resultado que el tráfico de upstream circule a través de la interfaz 200.1.1.20/32 considerada como Principal. En esta prueba realizada los dos enlaces (Principal, Backup) a ISP1 se encuentran en estado DOWN.*

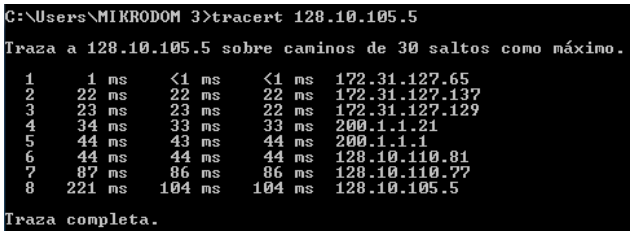


Figura 98 Pruebas BGP.

Realizado por: *Morales, W. 2016.*

- *Se procede a verificar alcanzabilidad entre un host ubicado en la interfaz fastethernet 0/1 de NY hacia el host localizado en la interfaz fastethernet 0/0 del router AMB ubicado en el AS100; dando como resultado que el tráfico de upstream circule a través de la interfaz 200.1.1.16/32 considerada como Principal. En esta prueba realizada todos los enlaces se encuentran en estado UP.*

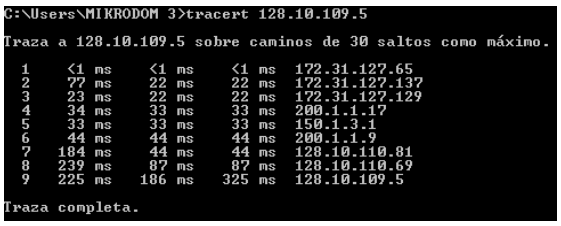


Figura 99 Pruebas BGP.

Realizado por: *Morales, W. 2016.*

- *Se procede a verificar alcanzabilidad entre un host ubicado en la interfaz fastethernet 0/1 de NY hacia el host localizado en la interfaz fastethernet 0/0 del router AMB ubicado en el AS100; dando como resultado que el tráfico de upstream circule a través de la interfaz 200.1.1.12/32 considerada como Backup. En esta prueba realizada todos los enlaces se encuentran en estado UP, excepto en Principal.*

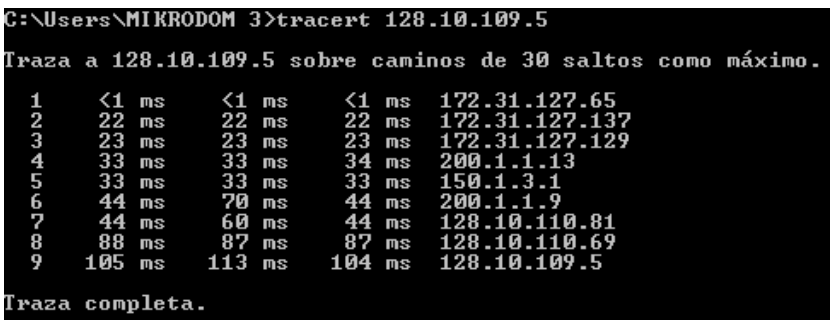


Figura 100 Pruebas BGP.

Realizado por: *Morales, W. 2016.*

- *Se procede a verificar alcanzabilidad entre un host ubicado en la interfaz fastethernet 0/1 de NY hacia el host localizado en la interfaz fastethernet 0/0 del router AMB ubicado en el AS100; dando como resultado que el tráfico de upstream circule a través de la interfaz 200.1.1.20/32 considerada como Secundario. En esta prueba realizada los dos enlaces (Principal, Backup) a ISP1 se encuentran en estado DOWN.*

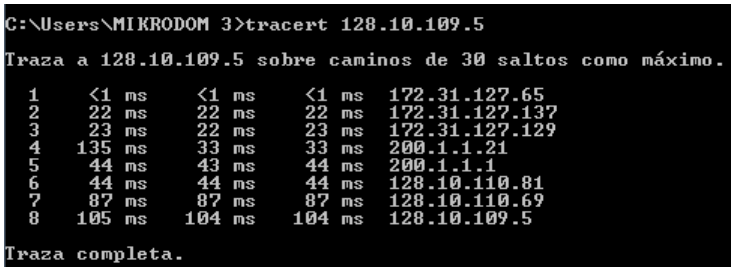


Figura 101 Pruebas BGP.

Realizado por: *Morales, W. 2016.*

6.4. Alta disponibilidad ASA

6.4.1.Rutas estáticas confiables

La redundancia y alta disponibilidad en los servicios IP es un tema que está en crecimiento en las redes de datos actuales, por lo que en el presente caso de estudio se analiza dos posibles escenarios; el primero usando el tracking de un objeto estático para medir el alcance de una ruta que se encuentra detrás de una interfaz física. Para este caso el tráfico generado desde el AS400 deberá salir por la interfaz Outside hacia el router WA para que se éste quien pueda enrutar los paquetes hacia redes remotas. ASA2 tiene cuatro interfaces Giga Ethernet que han sido configurados de la siguiente manera:

- *Giga Ethernet 0/0 la cual ha sido configurada con el Nameif "outside-1"*
- *Giga Ethernet 0/1 la cual ha sido configurada con el Nameif "outside-2"*
- *Giga Ethernet 0/2 la cual ha sido configurada con el Nameif "DMZ"*
- *Giga Ethernet 0/3 la cual ha sido configurada con el Nameif "Inside"*
- *Interface "outside-1" configurada un nivel de seguridad de 90*
- *Interface "outside-2" configurada un nivel de seguridad de 90*

- *Interface "DMZ" configurada un nivel de seguridad de 50*
- *Interface "Inside" configurada un nivel de seguridad de 0*

Para tener alta disponibilidad ASA se implementa en la arquitectura de red un mecanismo llamado "Rutas estáticas confiables" el cual permite atar una ruta estática con un objeto, la idea es que se haga una supervisión constante de ese objeto para saber si la ruta es o no alcanzable. Si dicho objeto se encuentra en estado de Up, se podrá confiar que la ruta estática también se encuentra en el mismo estado y por ende estará en la tabla de enrutamiento del ASA. Caso contrario, si el objeto está en un estado de Down el administrador de la red también sabrá que la ruta estático ya no se encuentra disponible y se sabrá que la ruta no estará presente en la tabla de enrutamiento.

El problema de tener un medio multiacceso como Ethernet para realizar esta tarea dificulta un poco, ya que si se ata una ruta estática a un objeto y éste viaja sobre este medio prácticamente se vería que siempre estará el objeto estará en up. En este caso se usará SLA (Service Level Agreement) con el fin de conocer si cierta dirección se mantiene o no activa.

La lógica es que si el SLA tiene alcanzabilidad con ese objeto que a su vez tiene una ruta estática se puede decir que realmente se tiene conexión con ese dispositivo y la ruta de mantendrá en la tabla de enrutamiento

Si por ejemplo el Firewall ASA2 estaría conectado a un switch metro Ethernet que a su vez tenga múltiples proveedores de servicio; si la red de uno de los proveedores deja de funcionar por cualquier razón, siempre se vería que la ruta sigue siendo alcanzable ya que estamos conectados a un medio multiacceso como Ethernet.

```
WA#debug ip icmp
ICMP packet debugging is on
WA#
*May  6 08:23:41.415: ICMP: echo reply sent, src 172.31.127.129, dst 172.31.127.130
WA#
*May  6 08:23:46.415: ICMP: echo reply sent, src 172.31.127.129, dst 172.31.127.130
WA#
*May  6 08:23:51.415: ICMP: echo reply sent, src 172.31.127.129, dst 172.31.127.130
WA#
*May  6 08:23:56.415: ICMP: echo reply sent, src 172.31.127.129, dst 172.31.127.130
```

Figura 102 Debugging ICMP-WA.

Realizado por: *Morales, W. 2016.*

El SLA es el responsable de enviar paquetes ICMP al dispositivo que se necesita hacer tracking, es este caso a la dirección 172.31.127.129. Para esto se necesita de un track que haga el seguimiento permanente del SLA; mientras haya respuesta a los paquetes ICMP el track seguirá en estado up

Requerimiento:

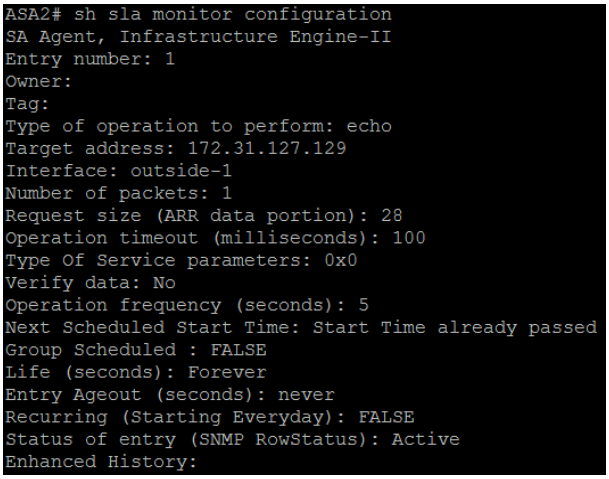


Figura 103 Verificación SLA-ASA2.

Realizado por: *Morales, W. 2016.*

Se puede definir la cantidad de paquetes que pueden ir de prueba en cada Segundo usando el comando ***frecuency*** *o se puede configurar el número de paquetes a enviarse así como un threshold en lo cual serviría para afinar un poco más la configuración. Se puede usar el comando time-out para definir cuál es el tiempo máximo para considerar una pérdida de conexión, etc.*

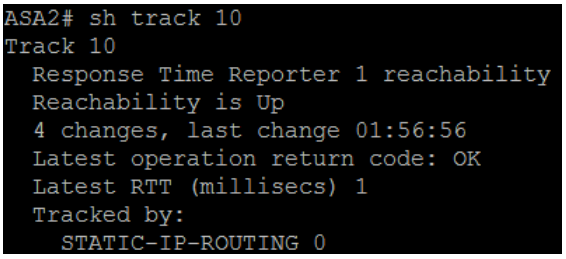


Figura 104 Estado del track-ASA2.

Realizado por: *Morales, W. 2016.*

Para temas de t-shoot es recommendable el uso de este commando ***show track [x]*** *ya que la salida "Latest operation return code" muestra cual es el estado del proceso, en este caso OK.*

```
ASA2# show running-config route
route outside-1 0.0.0.0 0.0.0.0 172.31.127.129 1 track 10
route outside-2 0.0.0.0 0.0.0.0 172.31.127.149 2
```

Figura 105 Rutas estáticas-ASA2.

Realizado por: *Morales, W. 2016.*

Se puede observar que el track se encuentra dando seguimiento a la dirección 172.31.127.129, si por alguna razón dicha interfaz se cae esto se verá reflejado en la tabla de enrutamiento. En este caso podemos observar que hay un Gateway por defecto apuntando 172.31.127.129 haciendo que esa sea la interfaz que tenga prioridad para el envío de paquetes ya que la distancia administrativa de una ruta estática tiene prioridad sobre otras.

Cuando por alguna razón no se tiene conectividad hacia el objeto, la ruta estática deja ser alcanzable y por ende entra a funcionar la ruta flotante que tiene una métrica de 2 la cual que no ingresa a la tabla de enrutamiento hasta que la principal haya caído.

```
ASA2# sh route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 172.31.127.129 to network 0.0.0.0

O E2 172.31.127.140 255.255.255.252
           [110/20] via 172.31.127.154, 1:57:24, inside
O    172.31.127.136 255.255.255.252
           [110/74] via 172.31.127.154, 1:57:24, inside
O    172.31.127.132 255.255.255.252
           [110/74] via 172.31.127.154, 1:57:24, inside
C    172.31.127.128 255.255.255.252 is directly connected, outside-1
C    172.31.127.152 255.255.255.252 is directly connected, inside
C    172.31.127.148 255.255.255.252 is directly connected, outside-2
O    172.31.127.144 255.255.255.252
           [110/11] via 172.31.127.149, 1:57:24, outside-2
O    172.31.122.0 255.255.254.0
           [110/11] via 172.31.127.149, 1:57:24, outside-2
O E2 172.31.127.0 255.255.255.192 [110/20] via 172.31.127.154, 1:15:49, inside
C    192.168.2.0 255.255.255.0 is directly connected, dmz
O E2 30.4.4.4 255.255.255.255 [110/20] via 172.31.127.154, 1:57:26, inside
O    30.5.5.5 255.255.255.255 [110/11] via 172.31.127.149, 1:57:26, outside-2
O E1 30.2.2.2 255.255.255.255 [110/110] via 172.31.127.154, 1:57:26, inside
O E2 30.3.3.3 255.255.255.255 [110/20] via 172.31.127.154, 1:57:26, inside
O    30.1.1.1 255.255.255.255 [110/11] via 172.31.127.129, 1:57:26, outside-1
S*   0.0.0.0 0.0.0.0 [1/0] via 172.31.127.129, outside-1
```

Figura 106 Tabla de enrutamiento-ASA2.

Realizado por: *Morales, W. 2016.*

Una vez que no responde el track de la primera ruta estática que tiene una métrica de 1 [172.31.127.129], enseguida ingresa en la tabla de enrutamiento la ruta estática que tiene una

métrica de 2 [172.31127.149] no se pierde conectividad en la topología. Este ejemplo de configuración se puede implementar cuando se tenga Multi-homing entre varios proveedores de servicio. Con esto queda demostrado que se levanta una ruta inmediatamente cuando no se detecta que hay respuesta del track que sigue el objeto; ofreciendo de esta forma alta disponibilidad en ASA.

```
ASA2# sh route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 172.31.127.149 to network 0.0.0.0

O E2 172.31.127.140 255.255.255.252
           [110/20] via 172.31.127.154, 0:00:21, inside
O    172.31.127.136 255.255.255.252
           [110/74] via 172.31.127.154, 0:00:21, inside
O    172.31.127.132 255.255.255.252
           [110/74] via 172.31.127.154, 0:00:21, inside
C    172.31.127.152 255.255.255.252 is directly connected, inside
C    172.31.127.148 255.255.255.252 is directly connected, outside-2
O    172.31.127.144 255.255.255.252
           [110/11] via 172.31.127.149, 0:00:21, outside-2
O    172.31.122.0 255.255.254.0
           [110/11] via 172.31.127.149, 0:00:21, outside-2
O E2 172.31.127.0 255.255.255.192 [110/20] via 172.31.127.154, 0:00:21, inside
C    192.168.2.0 255.255.255.0 is directly connected, dmz
O E2 30.4.4.4 255.255.255.255 [110/20] via 172.31.127.154, 0:00:23, inside
O    30.5.5.5 255.255.255.255 [110/11] via 172.31.127.149, 0:00:23, outside-2
O E1 30.2.2.2 255.255.255.255 [110/110] via 172.31.127.154, 0:00:23, inside
O E2 30.3.3.3 255.255.255.255 [110/20] via 172.31.127.154, 0:00:23, inside
O    30.1.1.1 255.255.255.255 [110/12] via 172.31.127.149, 0:00:23, outside-2
S*   0.0.0.0 0.0.0.0 [2/0] via 172.31.127.149, outside-2
```

Figura 107 Tabla de enrutamiento-ASA2.

Realizado por: *Morales, W. 2016.*

6.4.2.Alta disponibilidad con interfaces redundantes

Este tipo de implementación permite tener una interfaz como Activa y otra en modo Standby, cuando una de ellas presente inconvenientes la interfaz que actúa como Standby tome el rol de Activa haciendo que se conmute inmediatamente el tráfico a la nueva interfaz activa

En la topología del presente caso de estudio se tiene que la interface Giga Ethernet 0/1 quedará configurada como Activa, mientras que la interface Giga Ethernet 0/2 quedará configurada Pasiva; de esta manera se incrementa y se mejora la disponibilidad en el servicio. Es importante re calcar que las propiedades de las interfaces físicas del switch S3 deben ser las mismas, si por alguna razón las interfaces de dicho switch son distintas no funcionará este

procedimiento ya que no podemos asociar una interfaz fastethernet como una interfaz Giga Ethernet.

Es necesario que las interfaces del ASA donde se implemente esta opción no tengan alguna configuración. Los pasos a seguir son los siguientes:

- *Primero se debe crear una interfaz lógica con el comando* ***interface redundant [1..8]***
- *Agregar las interfaces a la nueva interface redundante*
- *Configurar direccionamiento IP*
- *Nombre de las interfaces, así como los niveles de seguridad*
- *Se puede configurar que interface se desea que tome el rol de Activa*

```
ASA1# sh interface redundant 1
Interface Redundant1 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
        MAC address 001f.9e2b.9aa1, MTU 1500
        IP address 128.10.110.86, subnet mask 255.255.255.252
        4779 packets input, 2195527 bytes, 0 no buffer
        Received 2 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        1 L2 decode drops
        3267 packets output, 1207985 bytes, 0 underruns
        0 output errors, 0 collisions, 2 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops, 0 tx hangs
        input queue (curr/max packets): hardware (2/9) software (0/0)
        output queue (curr/max packets): hardware (0/2) software (0/0)
  Traffic Statistics for "outside":
        4778 packets input, 2109305 bytes
        3268 packets output, 1148641 bytes
        3306 packets dropped
      1 minute input rate 0 pkts/sec,  378 bytes/sec
      1 minute output rate 0 pkts/sec,  209 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  420 bytes/sec
      5 minute output rate 0 pkts/sec,  205 bytes/sec
      5 minute drop rate, 0 pkts/sec
  Redundancy Information:
        Member GigabitEthernet0/1(Active), GigabitEthernet0/2
        Last switchover at 22:28:02 UTC Dec 12 2016
```

Figura 108 Interface redundante-ASA1.

Realizado por: *Morales, W. 2016.*

Se puede observar en el gráfico que la interfaz redundante se encuentra activa y es usada por la interfaz "Outside" del Firewall ASA. En la parte inferior se puede apreciar en la informacion de redundancia que la interface Giga Ethernet 0/1 es la interfaz Activa y la Giga Ethernet 0/2 es la interfaz Standby

```
ASA1# sh running-config interface redundant 1
!
interface Redundant1
 member-interface GigabitEthernet0/1
 member-interface GigabitEthernet0/2
 nameif outside
 security-level 0
 ip address 128.10.110.86 255.255.255.252
```

Figura 109 Rutas estáticas-ASA2.

Realizado por: *Morales, W. 2016.*

En el gráfico se puede observar las interfaces que pertenecen al grupo redundante, donde se dan algunos detalles de la interfaz que está trabajando como Activa, en este caso la interfaz 128.10.110.86 cuya dirección IP es 128.10.110.84.

Para ejemplo demostrativo se realiza una conexión telnet entre los routers CCA y GYE, donde se muestra la tabla de conexiones del firewall ASA y se puede apreciar que la conexión la origina el router CCA con un puerto de conexión 25847

```
ASA1# show conn long
15 in use, 36 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, C - CTIQBE media, D - DNS, d - dump,
       E - outside back connection, F - outside FIN, f - inside FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, M - SMTP data, m - SIP media, n - GUP
       O - outbound data, P - inside back connection, p - Phone-proxy TFTP connection,
       q - SQL*Net data, R - outside acknowledged FIN,
       R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
       V - VPN orphan, W - WAAS,
       X - inspected by service module
UDP outside:10.1.1.21/161 (10.1.1.21/161) dmz:192.168.1.7/51332 (192.168.1.7/51332), flags -, idle 35s, uptime 35s, timeout 2m0s, bytes 126
UDP outside:10.1.1.21/161 (10.1.1.21/161) dmz:192.168.1.7/58784 (192.168.1.7/58784), flags -, idle 35s, uptime 35s, timeout 2m0s, bytes 174
TCP outside:10.1.1.21/23 (10.1.1.21/23) inside:128.10.110.81/25847 (128.10.110.81/25847), flags UIO, idle 17s, uptime 51s, timeout 1h0m, bytes 1238
UDP outside:10.1.1.21/161 (10.1.1.21/161) dmz:192.168.1.7/46652 (192.168.1.7/46652), flags -, idle 1m34s, uptime 1m34s, timeout 2m0s, bytes 130
UDP outside:10.1.1.21/161 (10.1.1.21/161) dmz:192.168.1.7/40249 (192.168.1.7/40249), flags -, idle 1m34s, uptime 1m34s, timeout 2m0s, bytes 174
TCP outside:10.1.1.21/179 (10.1.1.21/179) inside:10.1.1.17/63452 (10.1.1.17/63452), flags UIO, idle 2s, uptime 1h47m, timeout 1h0m, bytes 10190
TCP outside:190.152.43.106/22 (190.152.43.106/22) inside:128.10.109.130/63985 (128.10.109.130/63985), flags saA, idle 18s, uptime 27s, timeout 30s, bytes 0
TCP outside:190.152.43.106/22 (190.152.43.106/22) inside:128.10.109.130/63984 (128.10.109.130/63984), flags saA, idle 20s, uptime 29s, timeout 30s, bytes 0
UDP outside:192.168.2.12/5060 (192.168.2.12/5060) inside:128.10.109.130/63030 (128.10.109.130/63030), flags T, idle 2s, uptime 50m43s, timeout 2m0s, bytes 643029
UDP outside:192.168.2.12/0 (192.168.2.12/0) inside:128.10.109.130/63030 (128.10.109.130/63030), flags ti, idle 2m56s, uptime 2m56s, timeout 1m0s, bytes 0
```

Figura 110 Tabla de conexiones-ASA1.

Realizado por: *Morales, W. 2016.*

En el presente gráfico se puede evidenciar la tabla de conexiones del firewall ASA antes y después de hacer caer a propósito en enlace Activo sin que llegase a perjudicar en lo más mínimo la conexión telnet entre los routers; ya que se levantó inmediatamente la interfaz Standby. Con esto queda demostrado que la redundancia implementada en el Firewall funciona y es una excelente herramienta para alta disponibilidad

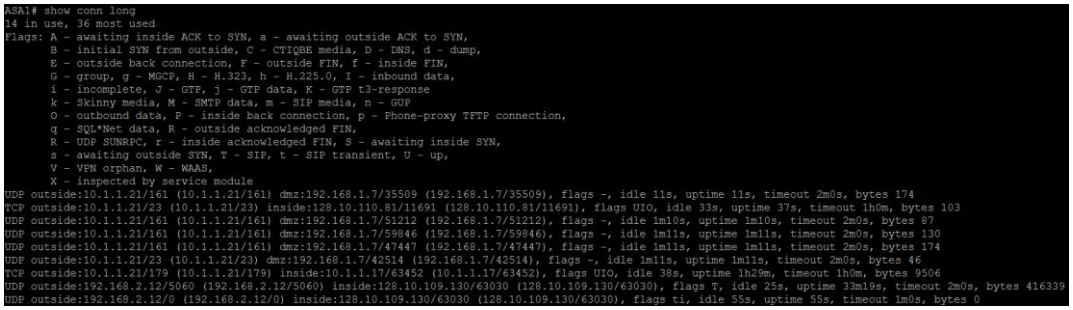


Figura 111 Tabla de conexiones al finalización sesión telnet-ASA1.

Realizado por: *Morales, W. 2016.*

Con la siguiente salida se puede observar que la dirección MAC de la interfaz redundante coincide con la interfaz Gi0/1 del ASA1. Si por ejemplo cayera la interfaz Gi0/1 del ASA1 entraría a trabajar como activa la interfaz GI0/2 y la interfaz redundante tendría la dirección MAC de Gi0/2.

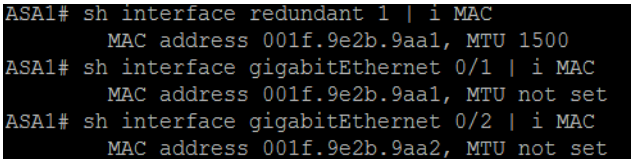


Figura 112 Direcciones MAC interfaces redundantes.

Realizado por: *Morales, W. 2016.*

En la siguiente salida se puede observar que al caer el enlace Gi0/1 quien toma el rol de Activo es la interfaz Gi 0/2.

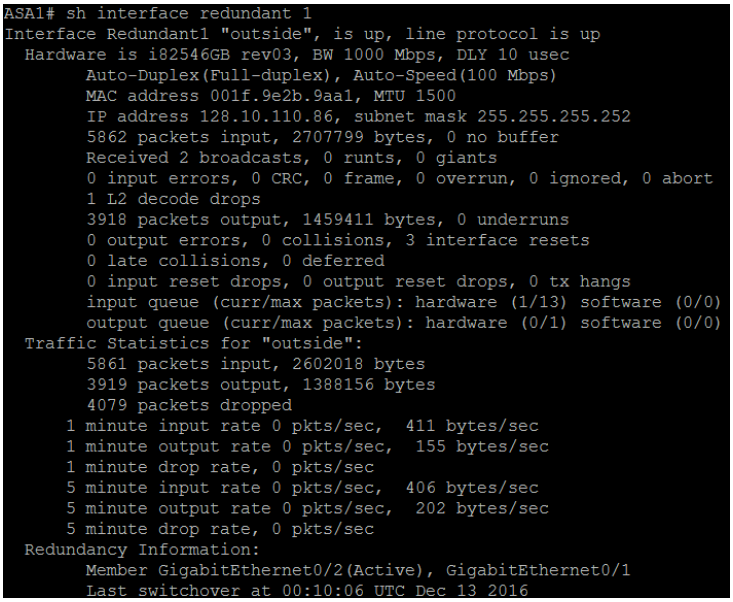


Figura 113 Interface redundante-ASA1.

Realizado por: *Morales, W. 2016.*

6.5. Redundancia LAN – GLBP

GLBP es un protocolo que en el presente caso de estudio se lo implementa con el fin de brindar redundancia a nivel de LAN, su funcionamiento en bastante parecido al de esus antecesores HSRP y VRRP; sin embargo este protocolo incorpora la posibilidad de realizar tareas de compartición de carga las cuales con sus antecesores no era posible

El router Active Virtual Gateway (AVG) será quien cumpla las tareas de orquestador en el grupo de GLBP; cada vez que llegan peticiones ARP para envío de tráfico éste contesta al cliente con la Mac address del equipo que se hará cargo de su petición. A diferencia de otros protocolos anteriores este escenario puede tener a múltiples routers encargados de atender los requerimientos que lleguen hasta el AVR. El AVR es escogido de acuerdo a quien poseea el mayor weight. En una topología se puede tener hasta 4 AVFs quienes son los encargados de solucionar las peticiones que llegan al AVG, es decir el tráfico se puede distribuir entre los 4. Tambien existe la posibilidad que un router sea AVG y AVF al mismo tiempo; por eso se puede hacer compartición de carga entre los cuatro equipos.

Los equipos que realmente van a estar haciendo forwarding de los paquetes serán los AVFs a menos que el AVG también colabore enrutando. En la topolgía de red el router LJA es AVG/AVF1 y el router IMB es AVF2, también se puede observar que tiene configurada subinterfaces en cada vlan de la LAN para hacer enrutamiento inter-vlan; asi como también el comando priority seteado en 150 para superar al valor por defecto para escoger al AVG, además especifica el peso inicial así como los umbrales que utilizará el gateway. Se configura el tracking de un objeto el valor que debe decrementar el peso cuando el tracking falle

```
interface FastEthernet0/1.10
 encapsulation dot1Q 10
 ip address 10.1.10.1 255.255.255.0
 no snmp trap link-status
 glbp 10 ip 10.1.10.254
 glbp 10 priority 150
 glbp 10 preempt
 glbp 10 weighting 110 lower 85 upper 105
 glbp 10 weighting track 15 decrement 30
```

```
interface FastEthernet0/1.10
 encapsulation dot1Q 10
 ip address 10.1.10.2 255.255.255.0
 no snmp trap link-status
 glbp 10 ip 10.1.10.254
 glbp 10 preempt
```

Figura 114 Track GLBP-LJA, IMB.

Realizado por: *Morales, W. 2016.*

En el gráfico se puede observar que para el grupo 10 en ambos routers, la prioridad es mayor en LJA por lo que es AVG/AVF y tiene un rol activo en la contestación de peticiones ARP. Lo contrario para IMB quién está de igual forma ayudando a la compratición de carga cuando el gateway requiera de su ayuda para direccionar paquetes fuera del grupo GLBP

```
LJA#sh glbp brief
Interface   Grp  Fwd Pri State    Address         Active router   Standby route
Fa0/1.10    10   -   150 Active   10.1.10.254     local           10.1.10.2
Fa0/1.10    10   1   7   Listen   0007.b400.0a01  10.1.10.2       -
Fa0/1.10    10   2   7   Active   0007.b400.0a02  local           -
Fa0/1.20    20   -   150 Active   10.1.20.254     local           10.1.20.2
Fa0/1.20    20   1   7   Listen   0007.b400.1401  10.1.20.2       -
Fa0/1.20    20   2   7   Active   0007.b400.1402  local           -
Fa0/1.30    30   -   150 Active   10.1.30.254     local           10.1.30.2
Fa0/1.30    30   1   7   Active   0007.b400.1e01  local           -
Fa0/1.30    30   2   7   Listen   0007.b400.1e02  10.1.30.2       -
Fa0/1.40    40   -   150 Active   10.1.40.254     local           10.1.40.2
Fa0/1.40    40   1   7   Listen   0007.b400.2801  10.1.40.2       -
Fa0/1.40    40   2   7   Active   0007.b400.2802  local           -
Fa0/1.100   100  -   150 Active   10.1.100.254    local           10.1.100.2
Fa0/1.100   100  1   7   Listen   0007.b400.6401  10.1.100.2      -
Fa0/1.100   100  2   7   Active   0007.b400.6402  local           -
LJA#
```

Figura 115 Tabla de conexiones-ASA1.

Realizado por: *Morales, W. 2016.*

```
IMB#sh glbp brief
Interface   Grp  Fwd Pri State    Address         Active router   Standby router
Fa0/1.10    10   -   100 Standby  10.1.10.254     10.1.10.1       local
Fa0/1.10    10   1   -   Active   0007.b400.0a01  local           -
Fa0/1.10    10   2   -   Listen   0007.b400.0a02  10.1.10.1       -
Fa0/1.20    20   -   100 Standby  10.1.20.254     10.1.20.1       local
Fa0/1.20    20   1   -   Active   0007.b400.1401  local           -
Fa0/1.20    20   2   -   Listen   0007.b400.1402  10.1.20.1       -
Fa0/1.30    30   -   100 Standby  10.1.30.254     10.1.30.1       local
Fa0/1.30    30   1   -   Listen   0007.b400.1e01  10.1.30.1       -
Fa0/1.30    30   2   -   Active   0007.b400.1e02  local           -
Fa0/1.40    40   -   100 Standby  10.1.40.254     10.1.40.1       local
Fa0/1.40    40   1   -   Active   0007.b400.2801  local           -
Fa0/1.40    40   2   -   Listen   0007.b400.2802  10.1.40.1       -
Fa0/1.100   100  -   100 Standby  10.1.100.254    10.1.100.1      local
Fa0/1.100   100  1   -   Active   0007.b400.6401  local           -
Fa0/1.100   100  2   -   Listen   0007.b400.6402  10.1.100.1      -
```

Figura 116 Configuración GLBP-IMB**.**

Realizado por: *Morales, W. 2016.*

Se puede observar que dentro del grupo 10 está la vlan que se utilizará para hará las respectivas pruebas de compartición de carga, se observa que el router LJA está en estado activo por lo que es el AVG pero también indica quién se encuentra en estado Standby con una prioridad de 100 (por defecto).

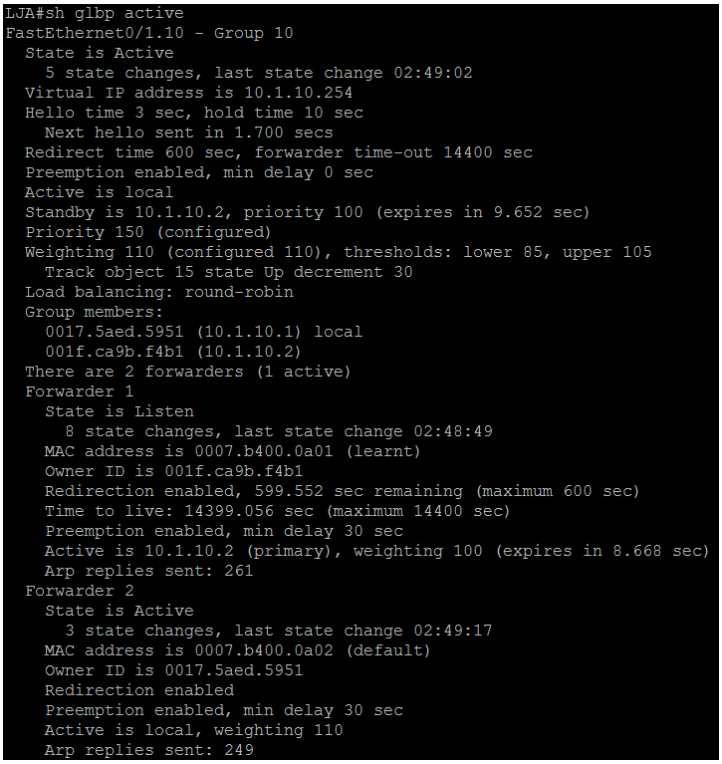


Figura 117 Información GLBP-LJA

Realizado por: *Morales, W. 2016.*

Se puede observar en la gráfica como LJA también actúa como AVF y conjuntamente con IMB hacer compartición de carga cuando se generan peticiones ARP. Con esto queda comprobado que a pesar que falle cualquiera de los dos equipos se tiene redundancia en la LAN con el uso de protocolo GLBP de Cisco y el seguimiento de objetos.

Figura 118 Compartición de carga-GLBP.

Realizado por: *Morales, W. 2016.*

7. Monitorear y generar alertas de tráfico vía correo electrónico y mensajes de texto (SMS) mediante el uso de una plataforma basada en Open Source y un circuito electrónico usando Microcontroladores PIC.

Una prueba más para comprobar el funcionamiento de la redundancia y alta disponibilidad que tiene la red, se opta por manitorear las interfaces seriales del router GYE con el objetivo de observar mediante gráficas elcomportamiento de la red cuando sobrepasa umbrales de tráfico establecidos por el administrador de la topologia.

Existen muchos programas dedicados al monitoreo de redes, sin embargo en el presente trabajo de titulación se optó por utilizar Cacti que es basado en Open Source, ademas que posee múltiples opciones descargando e instalando pluggins que en lo posterior serían de mucha utilidad para redes escalables. Cacti no solamente sirve para monitorear redes o borders como en el presente trabajo, sino más bien tiene una amplia gama de utilidades como el monitoreo de aplicaciones,servidores y diversos mecanismos que ayudan a laadministración de lsos procesos en ejecución. Existen muchas empresas que venden soluciones muy costosas y complejas de administrar, sin embargo estas tienen pocos días de vigencia sin costo como para probar el producto y familiarizarse. La desventaja de productos con licencias es que el precio de las mismas se van incrementando según la cantidad de nodos.

Nombre	Gráficas	Informes SLA	Grupos lógicos	Estadísticas	Predicción de estadísticas	Autodescubrimiento	Agentes	SNMP	Syslog	Scripts externos	Complementos (plugins)	Creación de complementos	Alertas	Aplicación web	Monitorización distribuida	Método de almacenaje de datos	Licencia	Mapas	Seguridad	Eventos
I-enable nnf	✓ Si	✓ Si	✓ Si	✓ Si	✓ Si	✓ Si	✓ Con agente y sin agente	✓ Si	✓ Si	✓ Si	✓ Si	Fácil	✓ Si	✓ Control total	✓ Si	MySQL y Berkeley DB	Comercial	✓ Si	✓ Si	✓ Si
Pandora FMS	✓ Si	✓ En tiempo real o programados	✓ Si	✓ Si	✓ Si	✓ Si	✓ Con agente y sin agente	✓ Si	✓ Si	✓ Si	✓ Si	Fácil	✓ Si	✓ Control total	✓ Si	MySQL,Oracle	GPL Comercial	✓ Mapas de red automáticos y definibles por el usuario con edición interactiva	✓ Control de acceso granular afinado	✓ Si
Entuity	✓ Si	✓ Si	✓ Si	✓ Si	✓ Si	✓ Si	✗ No	✓ Si	✓ Si	✓ Si	✓ Si	Media	✓ Si	✓ Control total (incl. clientes Java)	✓ Si	MySQL	Comercial	✓ Dynamic/Personalizable	✓ Control de acceso granular afinado	✓ Si
Nimsoft	✓ Si	✓ Si	✓ Si	✓ Si	✓ Si	✓ Si	✓ Con agente y sin agente	✓ Si	✓ Si	✓ Si	✓ Si	Media	✓ Si	✓ Control total	✓ Si	SQL	Comercial	✓ Pantallas dinámicas y personalizables	✓ Control granular de acceso	✓ Si
Netscope	✓ Si	✓ Si	✓ Si	✓ Si	✓ Si	✓ Si	✓ Si	✓ Si	✓ Si	✓ Si	✓ Si	No	✓ Si	✓ Control total	✓ Si	SQL	Comercial	Desconocido	Desconocido	Desconocido
Zyrion	✓ Si	✓ En tiempo real o programados	✓ Si	✓ Si	✓ Si	✓ Si	✓ Con agente o sin agente	✓ Si	✓ Si	✓ Si	✓ Si	Fácil	✓ Si	✓ Control total	✓ Si	SQL	Comercial	✓ Personalizable	✓ Roles	✓ Si
PacketTrap	✓ Si	✗ No	✓ Si	✓ Si	Desconocido	✓ Si	✓ Si	✓ Si	✓ Si	✓ Si	✓ Si	Media	✓ Si	✓ Visualización e informes	✓ Si	SQL	Comercial	Desconocido	Desconocido	Desconocido
Big Brother	Desconocido	Desconocido	Desconocido	Desconocido	Desconocido	Desconocido	Desconocido	Desconocido	Desconocido	Desconocido	Desconocido	Desconocido	Desconocido	Desconocido	Desconocido	Desconocido	Comercial	Desconocido	Desconocido	Desconocido
dopplerVUE	✓ Si	✓ Si	✓ Si	✓ Si	✓ Si	✓ Si	✗ No	✓ Si	✓ Si	✓ Si	✓ Si	Ensamblador .NET	✓ Si	✓ Control total	✓ Si	SQL	Comercial	✓ Dynamic & Personalizable plus overlays	✓ Si	✓ Si
CA eHealth	✓ Si	✓ Si	✓ Si	✓ Si	✓ Si	✗ No	✓ Si	✓ Si	Con agente SystemEDGE	Con agente SystemEDGE	✗ No	Desconocido	✓ Si	✓ Reporting, Limited configuration	✓ Si	Oracle	Comercial	✗ No	✓ Control granular de acceso	✓ Si
Nagios	✓ Si	✓ Si	✓ Si	✓ Si	✓ Si	✓ Si	✓ Si	✓ A través de plugin	✓ Si	✓ Si	✓ Si	Media	✓ Si	Solo visualización	✓ Si	SQL	GPL	Desconocido	Desconocido	Desconocido
LoriotPro	✓ Si	✓ Si	✓ Si	✓ Si	✓ Si	✓ Si	✓ Si	✓ Si	✓ Si	✓ Si	✓ Si	✓ Si	✓ Si	✓ Si	✓ Si	Archivos de texto plano/SQL	Comercial/Libre	✓ Si Active View	✓ Si	✓ Si
Ganglia	✓ Si	Desconocido	✓ Si	Desconocido	Desconocido	✓ A través de comprobación gmond	✓ Si	✓ A través de plugin	✓ Si	✓ Si	✓ Si	Media	✓ Si	Solo visualización	✓ Si	RRDtool, en memoria	GPL	✓ Si	✓ Si	✓ Si
op5 Monitor	✓ Si	✓ Si	✓ Si	✓ Si	✓ Si	✓ Si	✓ Si	✓ Si	✓ Si	✓ Si	✓ Si	Fácil	✓ Si	✓ Control total	✓ Si	SQL	Comercial	✓ Si	✓ Si	✓ Si
Zabbix	✓ Si	✓ Si	✗ No	✓ Si	✓ Si	✓ Si	✓ Si	✓ Si	✓ Si	✓ Si	✓ Si	Fácil	✓ Si	✓ Control total	✓ Si	SQL	GPL	✓ Si	✓ Si	✓ Si
Munin	✓ Si	✓ Si	✓ Si	✓ Si	Desconocido	✓ Si	✓ Si	✓ Si	✓ Si	✓ Si	✓ Si	Media	SQL	Solo visualización, vía CGI/XML	Desconocido	RRDtool	GPL	Desconocido	Desconocido	Desconocido
Cacti	✓ Si	✓ Si	✓ Si	✓ Si	✗ No	✓ A través de plugin	✓ Si	✓ Si	✓ Si	✓ Si	✓ Si	Media	✓ Si	✓ Control total	✗ No	RRDtool y MySQL	GPL	✓ A través de plugin (Weathermap)	✓ Roles personalizados	✗ No se tiene plugin
Zenoss	✓ Si	✗ No	✓ Si	✓ Si	✓ Si	✓ Si	✓ SNMP, WMI, JMX, etc.	✓ Si	✓ Si	✓ Si	✓ Si	Fácil	✓ Si	✓ Control total	✓ Si	RRDtool y MySQL	GPL	✓ Si	✓ Si	✓ Si
Berkeley DB	Licencia artística	✗ No	✓ Granular afinado	✓ Si																
Hobbit Monitor Llamado ahora Xymon	✗ No	✓ Si	✓ Si	✓ Si	✗ No	✗ No	✓ Linux, Solaris, BSD, *NIX, Windows	✓ Si	✓ Si	✓ Si	✓ Si y soporta BB	Fácil	✓ Si	✓ Viewing, acknowledging, limited configuring	✓ Si	Archivos de texto plano y RRDtool	GPL	✗ No	✗ No	✓ Si
ManageEngine OpManager	✓ Si	Desconocido	✓ Si	✓ Si	✗ No	✓ Si	✗ No	✓ Si	Desconocido	✓ Si	✓ Si	Fácil	✓ Si	✓ Control total	✓ Si	MySQL y MSQL	Comercial: disponible versión libre con 10 nodos	Desconocido	Desconocido	Desconocido
OpenNMS	✓ Si	✓ Si	✗ No	✓ Si	Desconocido	✓ Si	✓ SNMP, WMI, JMX, usando WMIPE	✓ Si	✓ Si	✓ Si	✓ Si	Media	✓ Enrutamiento, escalas y horarios	✓ Control total	✓ cliente mínimo o snmp proxy	jrobin, RRDtool y PostgreSQL	GPL	✓ Pantallas dinámicas con Svg	✓ LDAP y Pantallas con dashboard	✓ Si
Fire Scope BSM: BE	✓ Si	✓ Si	✓ Si	✓ Si	✓ Si	✓ Si	✓ Con agente y sin agente	✓ Si	✓ Si	✓ Si	✓ Si	Fácil	✓ Si	✓ Control total	✓ Si	SQL	Comercial	Desconocido	Desconocido	Desconocido

Figura 119 Compartición de carga-GLBP.

Fuente: *https://blog.pandorafms.org/es/herramientas-de-monitoreo-de-redes/*

Cacti tiene un espacio para introducir scripts, esto es de gran ventaja ya que no es un sistema cerrado sino mas bien el alcance del monitoreo de la red queda cerrado a experticia que tenga el administrador de la red para crear dichos scripts. Existen sistemas que no tienen de forma gratuita el envío de alertas, en Cacti mediante el uso de datos seriales y un circuito electrónico acoplado, se pueden crear alertas via SMS.

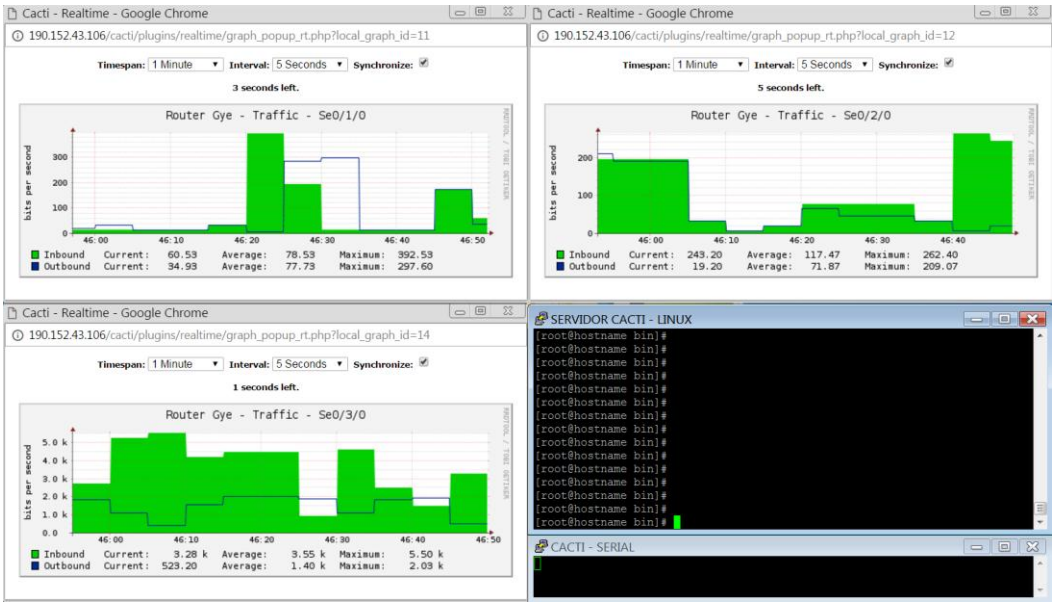


Figura 120 Compartición de carga-GLBP.

Realizado por: *Morales, W. 2016.*

El servidor Cacti se encuentra dentro de la DMZ del firewall ASA1 en el AS100, la idea es que se encuentre en un lugar que no sea susceptible a ataques provenientes de la red, es por eso motivo que se encuentra en la zona desmilitarizada del firewall. El servidor podrá monitorear los 3 enlaces que comunican el AS100 con el resto de la topología. Una limitante que se tuvo fue la poca capacidad de los enlaces, esto se vio reducido a trabajar con una baja tasa de transmisión de datos no mayores a 175 kbps. No se pudieron realizar los cambios necesarios, ya que las adyacencias entre la mayoría de los routers de la topología de red fueron hechos con enlaces WAN de baja velocidad, y la tasa de transmisión quedó limitada al hardware de los routers y al Clock-Rate máximo que se puede configurar en cada uno de ellos.

El script está diseñado de tal forma que simule una acción cuando sobrepase un threshold determinado cuando el tráfico circule por una interfaz. Estos son los requerimientos.

Interfaz	***Serial 0/3/0***
Threshold	*Superior a: 90 kbps*
Acción 1	*Conmutación de tráfico a serial 0/2/0*
Acción 2	*Envío de alerta vía correo electrónico al administrador*
Acción 3	*Envío de dato serial: "A"*

Tabla 1 Envío de notificaciones vía correo electrónico

Realizado por: *Morales, W. 2016.*

Figura 121 Script para envío de notificaciones vía correo electrónico.

Realizado por: *Morales, W. 2016.*

En esta imagen se puede apreciar la parte de las acciones que ejecuta Cacti cuando sobrepasa el umbral establecido

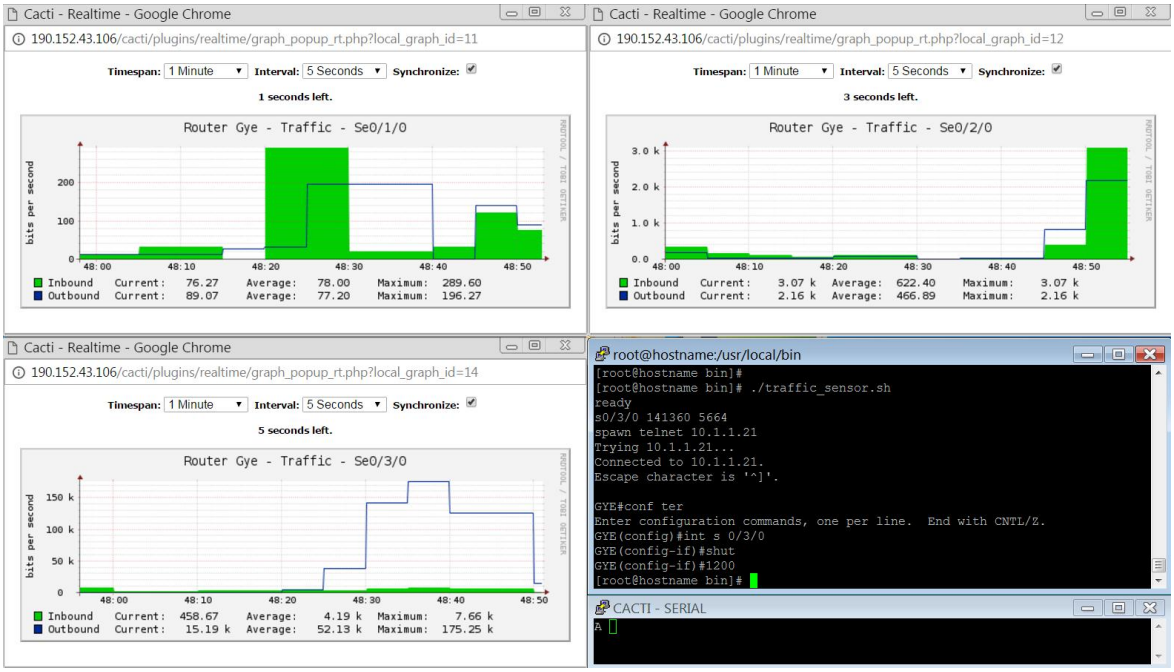


Figura 122 Envío de tráfico a se 0/2/0

Realizado por: *Morales, W. 2016.*

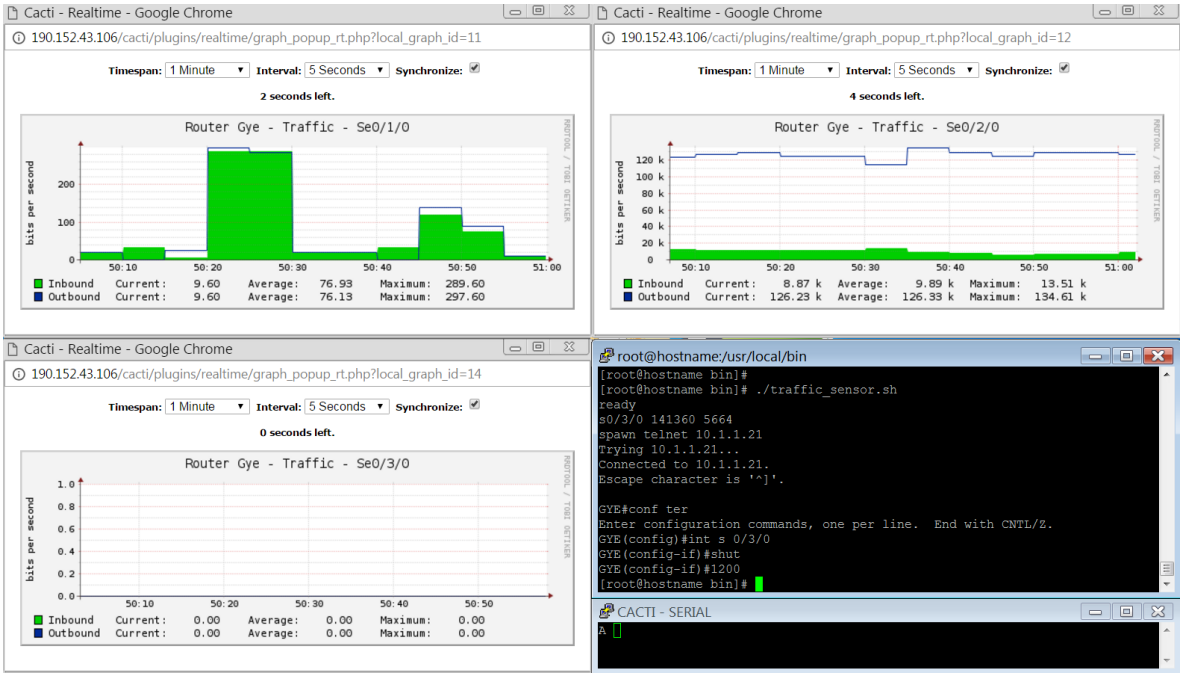


Figura 123 Envío de tráfico a se 0/2/0

Realizado por: *Morales, W. 2016.*

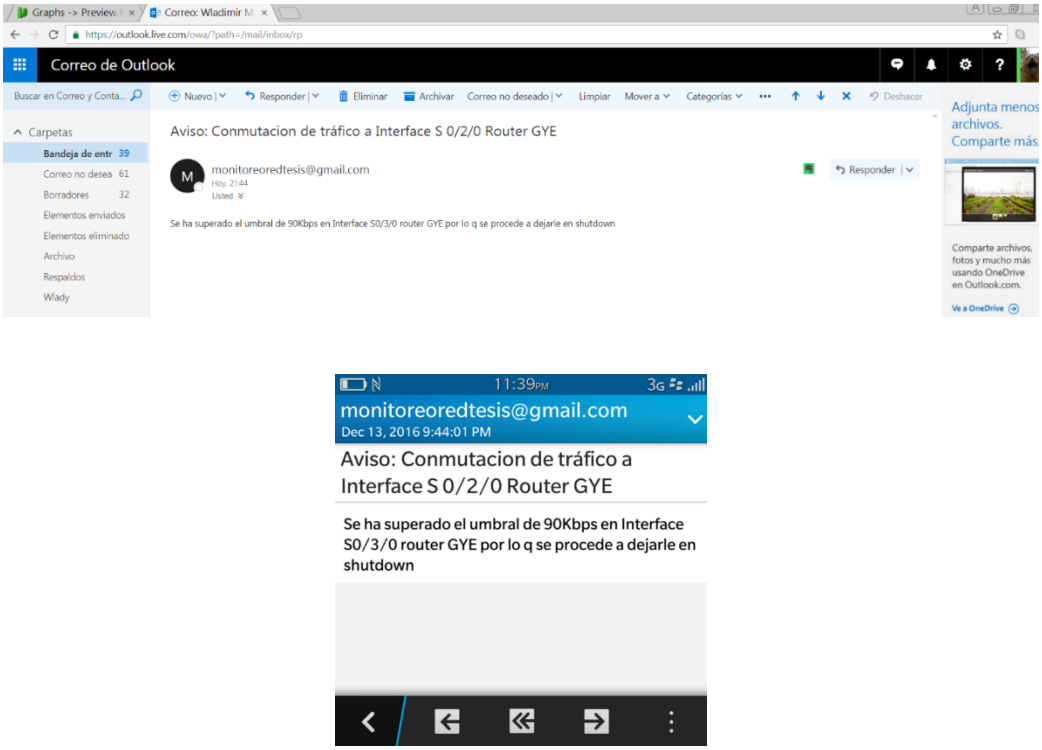


Figura 124 Envío de tráfico a se 0/2/0

Realizado por: *Morales, W. 2016.*

Interfaz	***Serial 0/2/0***
Threshold	*Superior a: 125 kbps*
Acción 1	*Conmutación de tráfico a serial 0/1/0*
Acción 2	*Envío de alerta vía correo electrónico al administrador*
Acción 3	*Envío de dato serial: "B"*

Tabla 2 Envío de notificaciones vía correo electrónico

Realizado por: *Morales, W. 2016.*

```
if [ "$Totals020out" -gt "125000" ] || [ "$Totals020in" -gt "125000" ]

        then
                echo "1" > /home/scripts/sensor/resultado/flags020.txt
                comando11=`echo -e "conf ter\nint s 0/2/0\nshut"`
                comando12=`echo -e "end\nexit\n"`
                #echo $comando1



                expect -c "
                        spawn telnet 10.1.1.21
                        sleep 5
                        expect \"\\\\GYE#\"
                        send \"$comando11\r\"
                        sleep 5
                        expect \"\\\\GYE(config-if)#\"
                        send \"$comando12\r\"
                        sleep 5
                        "
stty -F /dev/ttyS3 raw speed 1200
echo 'B' > /dev/ttyS3
echo  "Se ha superado el umbral de 125Kbps en Interface S0/2/0 router GYE por lo q se procede a dejarle en shutdown" | mail -s "Aviso: Conmutacion de trafico a Interface S 0/1/0 del Router
GYE" -r  monitoreoredtesis@gmail.com  animo-wlady@hotmail.com
```

Figura 125 Script para envío de notificaciones vía correo electrónico.

Realizado por: *Morales, W. 2016.*

En esta imagen se puede apreciar la parte de las acciones que ejecuta Cacti cuando sobrepasa el umbral establecido

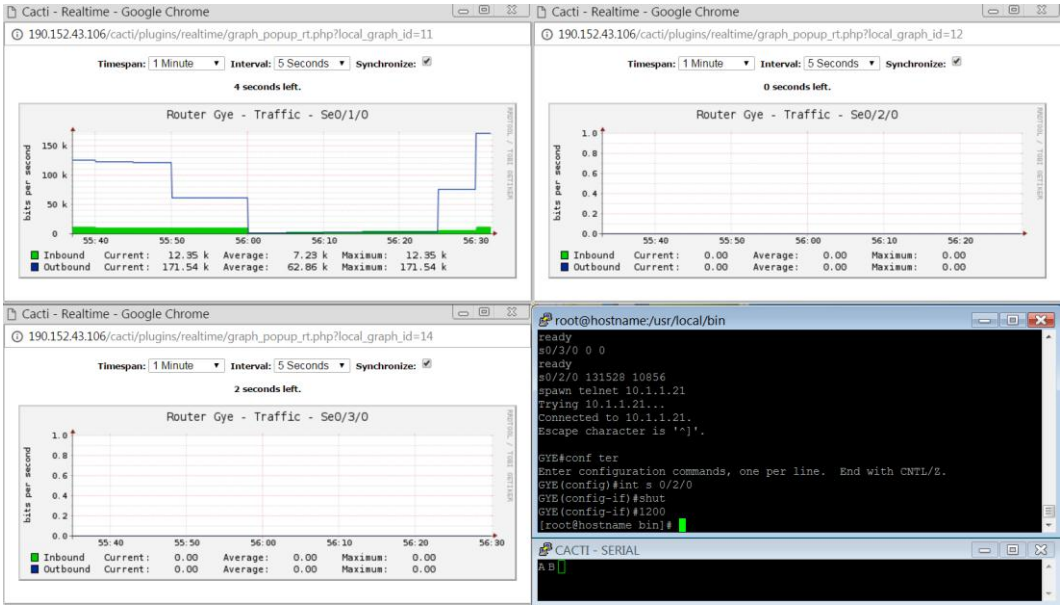


Figura 126 Envío de tráfico a se 0/1/0

Realizado por: *Morales, W. 2016.*

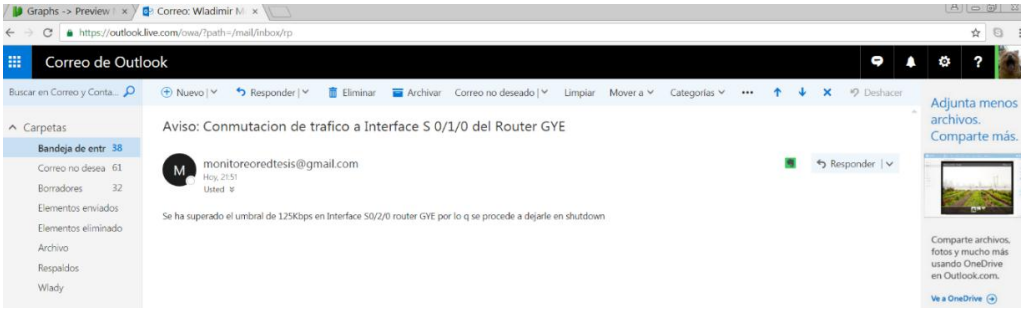


Figura 127 Envío de tráfico a se 0/2/0

Realizado por: *Morales, W. 2016.*

Interfaz	***Serial 0/1/0***
Threshold	*Inferior a: 126 kbps*
Acción 1	*Conmutación de tráfico a serial 0/2/0*
Acción 2	*Envío de alerta vía correo electrónico al administrador*
Acción 3	*Envío de dato serial: "C"*

Tabla 3 Envío de notificaciones vía correo electrónico

Realizado por: *Morales, W. 2016.*

Figura 128 Script para envío de notificaciones vía correo electrónico.

Realizado por: *Morales, W. 2016.*

En esta imagen se puede apreciar la parte de las acciones que ejecuta Cacti cuando sobrepasa el umbral establecido

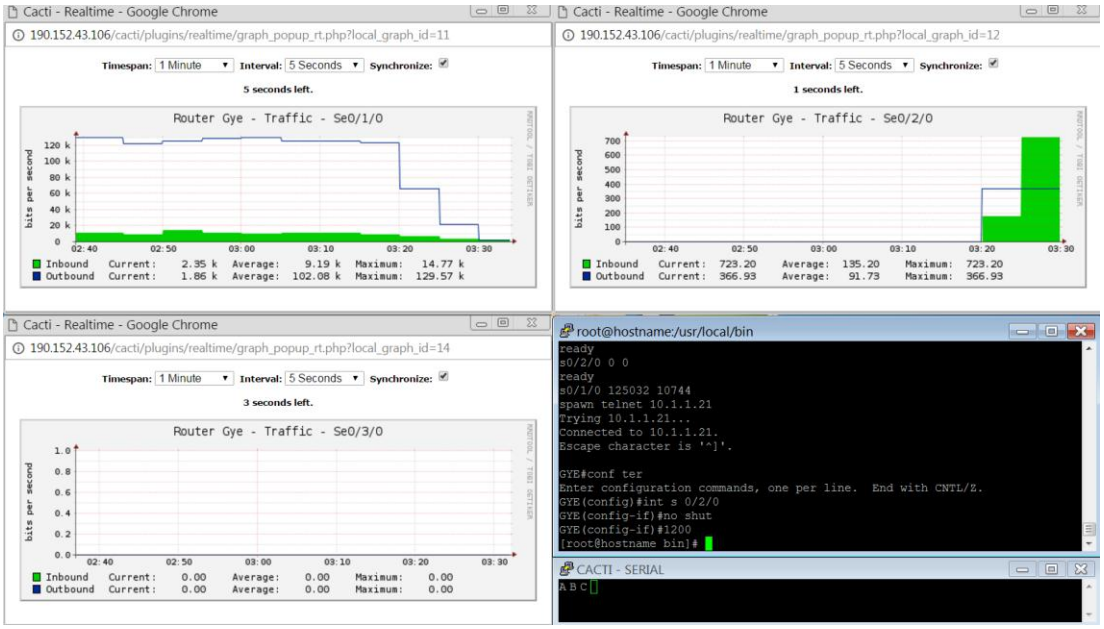


Figura 129 Envío de tráfico a se 0/2/0

Realizado por: *Morales, W. 2016.*

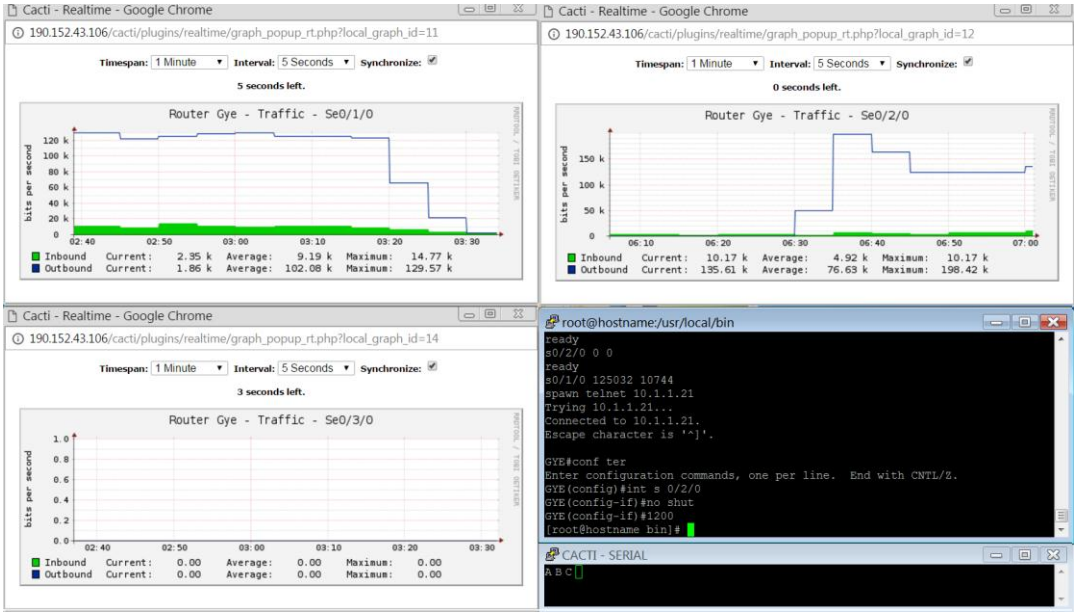


Figura 130 Envío de tráfico a se 0/2/0

Realizado por: *Morales, W. 2016.*

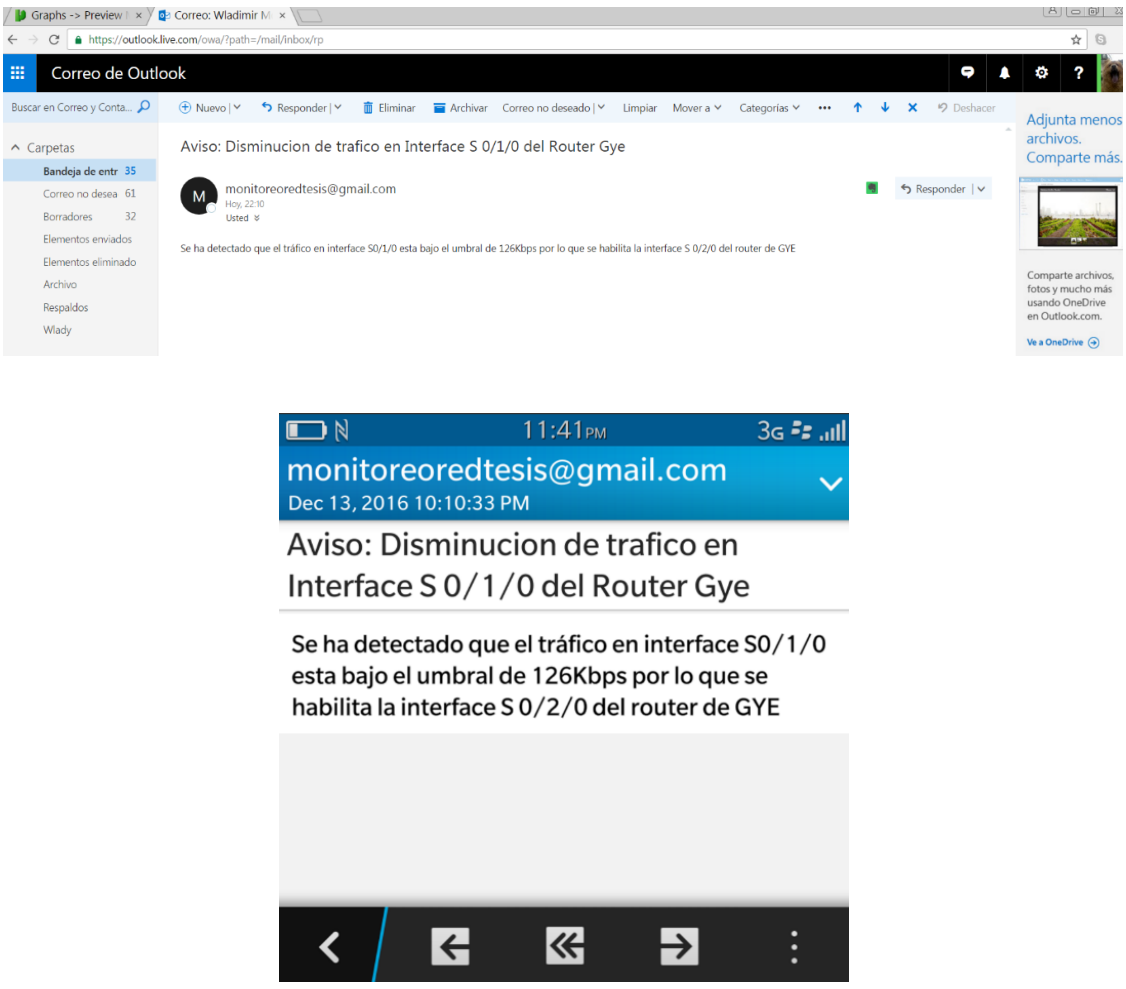


Figura 131 Envío de tráfico a se 0/2/0

Realizado por: *Morales, W. 2016.*

Interfaz	*Serial 0/2/0*
Threshold	*Inferior a: 110 kbps*
Acción 1	*Conmutación de tráfico a serial 0/3/0*
Acción 2	*Envío de alerta vía correo electrónico al administrador*
Acción 3	*Envío de dato serial: "D"*

Tabla 4 Envío de notificaciones vía correo electrónico

Realizado por: *Morales, W. 2016.*

Figura 132 Script para envío de notificaciones vía correo electrónico.

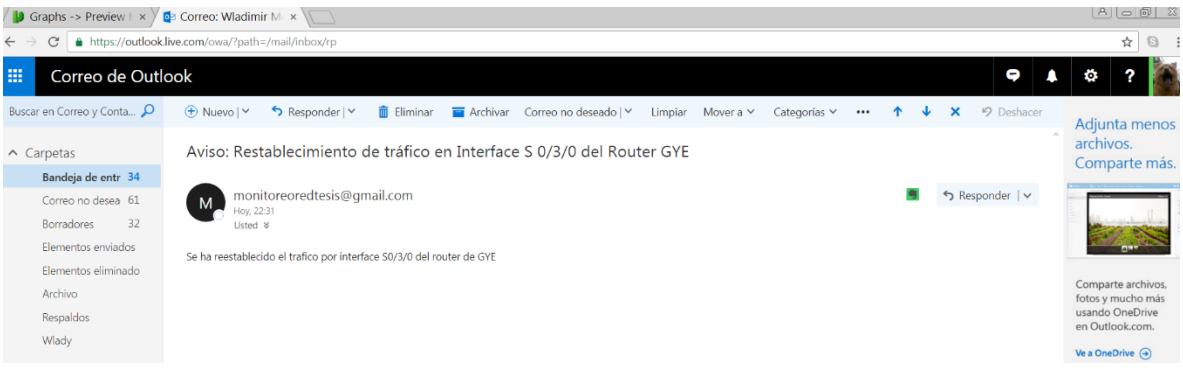
Realizado por: *Morales, W. 2016.*

En esta imagen se puede apreciar la parte de las acciones que ejecuta Cacti cuando sobrepasa el umbral establecido

La prueba consiste en enviar tráfico sftp desde el AS100 al AS400 y

Figura 133 Envío de tráfico a se 0/3/0

Realizado por: *Morales, W. 2016.*



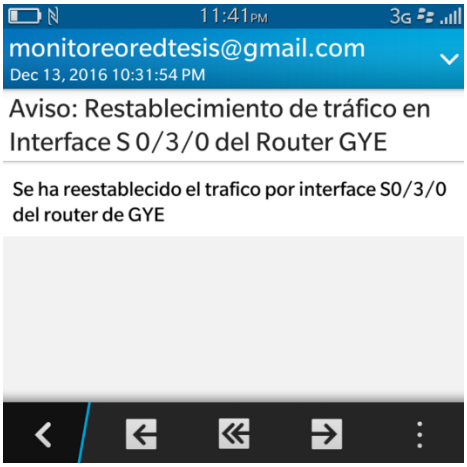


Figura 134 Envío de tráfico a se 0/2/0

Realizado por: *Morales, W. 2016.*

6.4.3.Notificaciones vía SMS

Con los datos obtenidos de la comunicación serial con el servidor Cacti, se procede a capturar vía serial toda la información en la memoria de un microcontrolador el cual procesará la información y éste a su vez se comunicará con un modem GSM para el envío de alertas al administrador de la red. Se diseñó la programación para que dependiendo del dato serial recibido pueda activar una salida con TRIAC o Relé; esto podría utilizarse para aplicaciones futuras donde sea necesario encender o apagar una carga.

Las pruebas se las realizará en un entrenador de aplicaciones universales de microcontroladores PIC, el uc usado es el PIC 16F819.

```
INI:
        SEROUT Tx_MODEM,  N1200,["AT",13,10]
        SERIN  Rx_MODEM,  N1200,5000,BAD,["OK"]
        SEROUT Tx_MODEM,  N1200,["AT+CMGF=1",13,10]
        SERIN  Rx_MODEM,  N1200,5000,BAD,["OK"]
        SEROUT Tx_MODEM,  N1200,["AT+CSCS=",34,"GSM",34,13,10]
;34 ES COMILLAS
        SERIN  Rx_MODEM,  N1200,5000,BAD,["OK"]
        GOTO PROG
BAD:
       lcdout $FE,$1, "     MODEM"
       lcdout $FE,$c0,"  NO RESPONDE"
FOR X = 1 TO 4
HIGH BUZZER
PAUSE 500
LOW BUZZER
PAUSE 100
NEXT X
'           lcdout $FE,$1, "   SISTEMA"
'           lcdout $FE,$c0,"  SIN MODEM"
```

Primero se debe setear la parte de la comunicación, en donde primero se envía un comando AT al modem GSM, si éste no responde se envía a una subrutina donde se podrá observar en la pantalla del LCD que no existe comunicación desde el microcontrolador hasta el módem. Este error puede ocurrir cuando no hay un chip de datos en el modem o que se encuentra apagado y no existe comunicación entre los dispositivos.

Si todo está correcto, se procede a setear el modo de trabajo del modem haciendo que se comunique usando modo texto y en la banda de transmisión GSM, no PDUs.

```
RX_SMS:
JMP_50:
        SERIN  Rx_PC,N1200,5000,JMP_50,DATO1
        IF DATO1 = "A" THEN
                        lcdout $FE,$1, "TRAFICO DIRIGIDO"
                        lcdout $FE,$c0,"      A: S2"
                        HIGH RELE
                        SEROUT Tx_PC,     N1200,["LETRA RECIBIDA:
A",13,10]
;                        SEROUT Tx_MODEM,  N1200,
["AT+CMGS=",34,"0997242736",34,13,10]
                        GOSUB TX_NUM
                        SERIN  Rx_MODEM,  N1200,1000,JMP_50,[">"]
                        SEROUT tx_MODEM,  N1200,["THRESHOLD
SUPERADO. TRAFICO CONMUTADO A INTERFACE SERIAL S2 DEL ROUTER GYE.
SALIDA 1 /ON",26,13,10]
                        SERIN  Rx_MODEM,  N1200,15000,JMP_50,
["OK"]
                        ENDIF
```

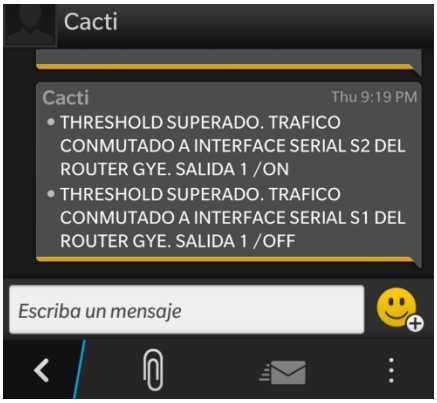


Figura 135 Envío de mensajes de texto SMS.

Realizado por: *Morales, W. 2016.*

Se espera cualquier datos serial proveniente del Servidor Cacti a una velocidad de 1200 bps, si es dato no es recibido por 5 segundos regresa a la subrutina de búsqueda de datos. Si encuentra un dato con la letra "A" entonces activa la visualización por la pantalla LCD, envía el mensaje de texto SMS y activa la salida que le corresponda.

```
        IF DATO1 = "B" THEN
                        lcdout $FE,$1, "TRAFICO DIRIGIDO"
                        lcdout $FE,$c0,"      A: S1"
                        LOW RELE
                        SEROUT Tx_PC,     N1200,["LETRA RECIBIDA:
B",13,10]
;                        SEROUT Tx_MODEM,  N1200,
["AT+CMGS=",34,"0997242736",34,13,10]
                        GOSUB TX_NUM
                        SERIN  Rx_MODEM,  N1200,1000,JMP_50,[">"]
                        SEROUT tx_MODEM,  N1200,["THRESHOLD
SUPERADO. TRAFICO CONMUTADO A INTERFACE SERIAL S1 DEL ROUTER GYE.
SALIDA 1 /OFF",26,13,10]
                        SERIN  Rx_MODEM,  N1200,15000,JMP_50,
["OK"]
                        ENDIF
```

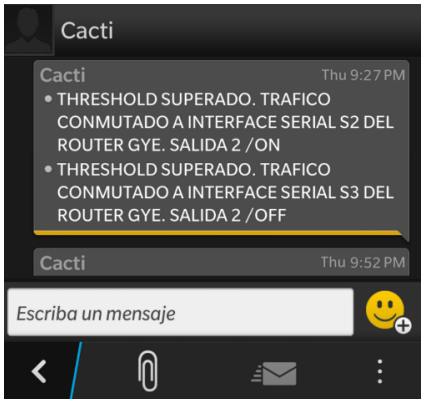


Figura 136 Envío de mensajes de texto SMS.

Realizado por: *Morales, W. 2016.*

Se espera cualquier datos serial proveniente del Servidor Cacti a una velocidad de 1200 bps, si es dato no es recibido por 5 segundos regresa a la subrutina de búsqueda de datos. Si encuentra un dato con la letra "B" entonces activa la visualización por la pantalla LCD, envía el mensaje de texto SMS y activa la salida que le corresponda.

```
        IF DATO1 = "C" THEN
                        lcdout $FE,$1, "TRAFICO DIRIGIDO"
                        lcdout $FE,$c0,"      A: S2"
                        HIGH TRIAC
                        SEROUT Tx_PC,     N1200,["LETRA RECIBIDA:
C",13,10]
;                        SEROUT Tx_MODEM,  N1200,
["AT+CMGS=",34,"0997242736",34,13,10]
                        GOSUB TX_NUM
                        SERIN  Rx_MODEM,  N1200,1000,JMP_50,[">"]
                        SEROUT tx_MODEM,  N1200,["THRESHOLD
SUPERADO. TRAFICO CONMUTADO A INTERFACE SERIAL S2 DEL ROUTER GYE.
SALIDA 2 /ON",26,13,10]
                        SERIN  Rx_MODEM,  N1200,15000,JMP_50,
["OK"]
                        ENDIF
```

Se espera cualquier datos serial proveniente del Servidor Cacti a una velocidad de 1200 bps, si es dato no es recibido por 5 segundos regresa a la subrutina de búsqueda de datos. Si encuentra un dato con la letra "C" entonces activa la visualización por la pantalla LCD, envía el mensaje de texto SMS y activa la salida que le corresponda.

```
        IF DATO1 = "D" THEN
                        lcdout $FE,$1, "TRAFICO DIRIGIDO"
                        lcdout $FE,$c0,"      A: S3"
                        LOW TRIAC
                        SEROUT Tx_PC,     N1200,["LETRA RECIBIDA:
D",13,10]
;                        SEROUT Tx_MODEM,  N1200,
["AT+CMGS=",34,"0997242736",34,13,10]
                        GOSUB TX_NUM
                        SERIN  Rx_MODEM,  N1200,1000,JMP_50,[">"]
                        SEROUT tx_MODEM,  N1200,["THRESHOLD
SUPERADO. TRAFICO CONMUTADO A INTERFACE SERIAL S3 DEL ROUTER GYE.
SALIDA 2 /OFF",26,13,10]
                        SERIN  Rx_MODEM,  N1200,15000,JMP_50,
["OK"]
                        ENDIF
                        RETURN
```

Se espera cualquier datos serial proveniente del Servidor Cacti a una velocidad de 1200 bps, si es dato no es recibido por 5 segundos regresa a la subrutina en búsqueda de datos. Si

encuentra el dato serial "D" entonces activa la visualización por la pantalla LCD, envía el mensaje de texto SMS y activa la salida que le corresponda.

```
;*****************************************************
;*****************************************************
TX_NUM:
                          SEROUT Tx_MODEM,  N1200,
["AT+CMGS=",34,"0997242736",34,13,10]
                          RETURN
;*****************************************************
;*****************************************************
```

8. CONCLUSIONES

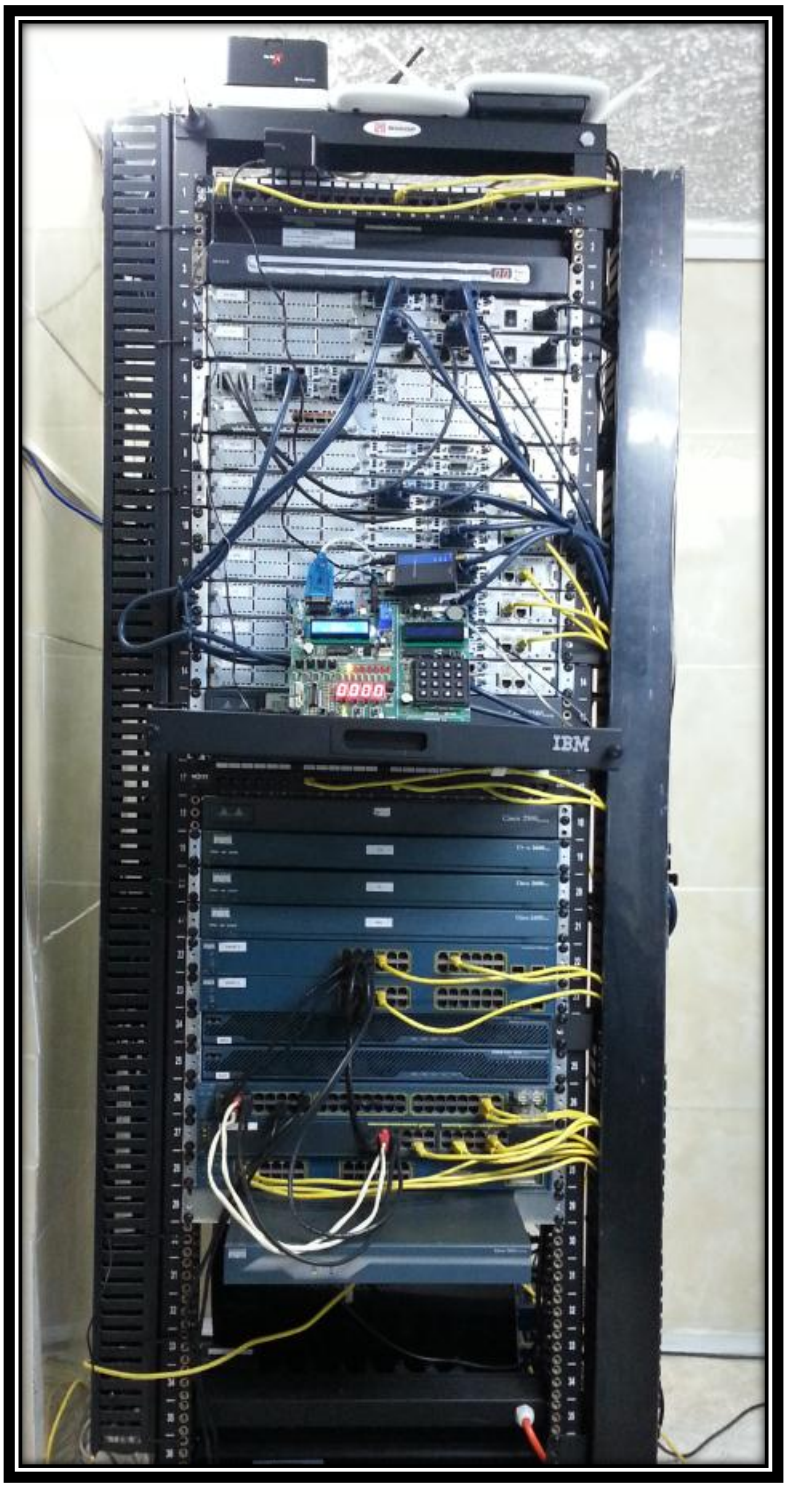
- *Con la realización del presente proyecto, se logró demostrar el uso del toolkit de cada protocolo y la convergencia de múltiples protocolos de enrutamiento dinámico usando redistribución de rutas.*
- *Se concluyó que para redes muy grandes y que sean compatibles entre distintas marcas dentro de un IGP, se deben usar protocolos de enrutamiento tales como IS-IS u OSPF.*
- *Los resultados alcanzados en las pruebas cumplieron el 100% de expectativas y objetivos iniciales, al proporcionar políticas de enrutamiento entre 2 sistemas autónomos públicos de 2 bytes con alta disponibilidad de enlaces.*
- *Se concluyó que en una red de producción real, es de suma importancia tener mecanismos como los analizados en el presente caso de estudio para alcanzar redundancia y alta disponibilidad que garanticen la continuidad del giro de negocio.*
- *Se investigó las diferentes posibilidades que se tiene en un Firewall ASA 5520 para brindar disponibilidad a la red cuando caigan las interfaces, siendo de alta efectividad.*
- *Se pudo fusionar a la topología mediante un script, un circuito electrónico de potencia basado en Microcontroladores PIC; el cual podría hacer que las posibilidades de monitoreo y acciones tomadas por un sistema en producción real sean cada vez mejores y más robustos.*
- *Los sistemas de monitoreo actuales ofrecen un alto costo. Mientras más grandes son los nodos, aumenta su valor por lo que el uso de herramientas Open Source como Cacti es cada vez más frecuente.*
- *Hay que estar conscientes que ningún prefijo de red puede ser anunciado a Internet por un Sistemas Autónomos privado, para hacerlo es necesario el enmascaramiento usando un AS Público.*

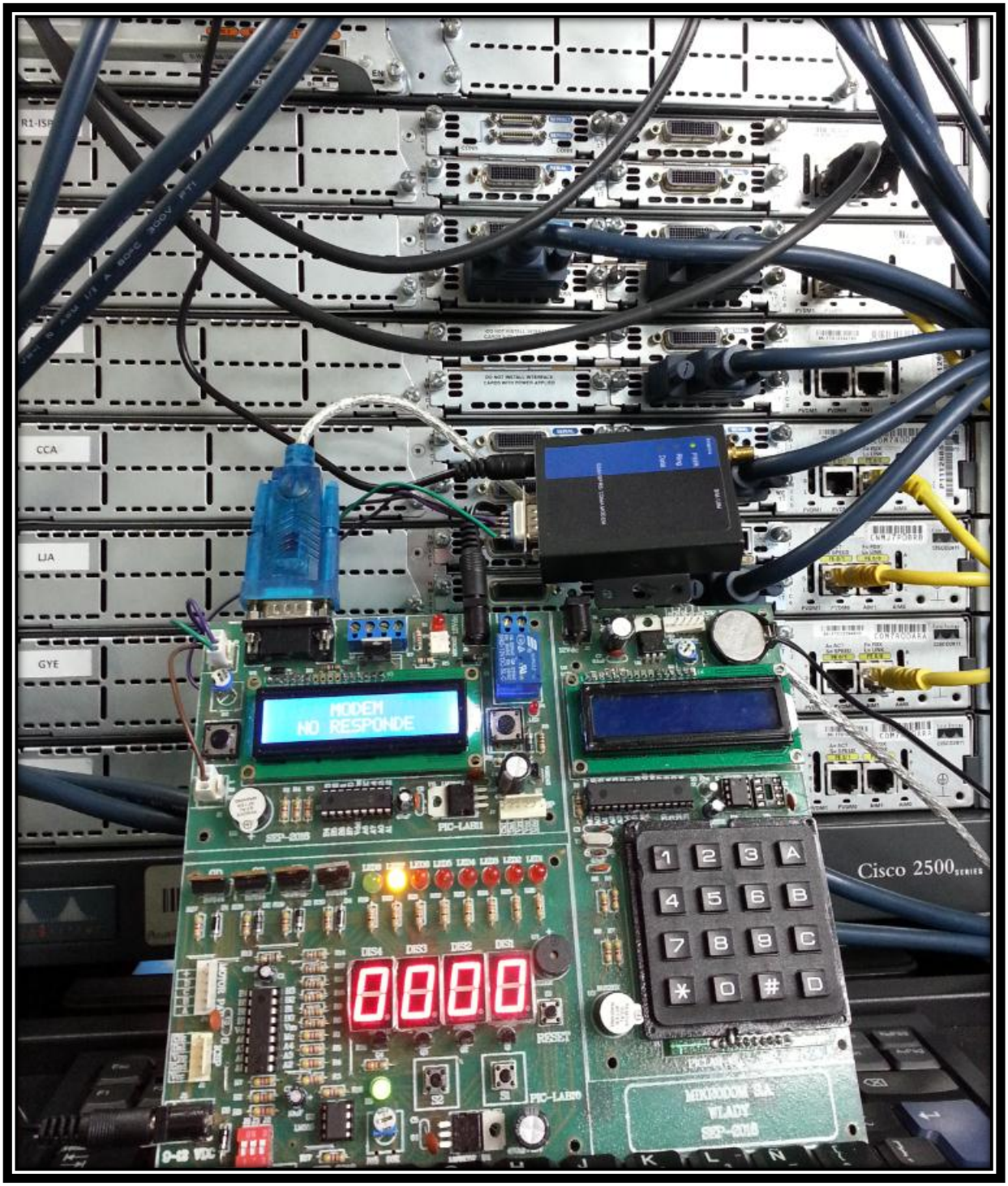
9. RECOMENDACIONES

- *En todo tipo de redes, especialmente si es escalable se recomienda la utilización de un esquema de direccionamiento basado en VLSM, con el objetivo de maximizar el uso y no desperdicio de direcciones IP.*
- *Configurar una lista de bogons dentro de las configuraciones de borde en un AS ayuda a evitar que se publiquen anuncios que no corresponder enviar a un ISP o Tier1.*
- *Se recomienda la utilización de sumarización en los equipos de borde del AS con rutas hacia interfaces NULL, con el objetivo de evitar fluctuaciones e inestabilidad en Internet.*
- *Se recomienda la utilización de Filtros tanto en sentido Inbound como Outbound en sesiones eBGP para evitar ser AS de Tránsito.*
- *Se recomienda utilizar como direcciones de Next-Hop para sesiones iBGP a interfaces Loopback, ya que no dependen del IGP ni del esquema de direccionamiento usado para levantar peerings.*
- *Se recomienda tener mucho cuidado en el uso de la función Dampening si se la utiliza, ya que los ISPs tienen tiempos de salida y penalizaciones muy altas, pudiendo hacer que la tabla de enrutamiento quede fuera de la visión de Internet hasta por 1 hora.*
- *Se recomienda que un ISP se asocie a un Punto de Intercambio regional, con el objetivo de no utilizar enlaces Internaciones.*
- *Es necesario el uso de RPKI en los routers que corresponden al ISP para comparar un determinado prefijo de red y sus capabilities con las políticas que se contrató. De esta forma se tendrá mayor control sobre los anuncios recibidos desde clientes.*
- *No se recomienda usar Confederaciones en sesiones eBGP ya que será necesaria la configuración de Sistemas Autónomos privados dentro del AS del cliente; llevando a configuraciones más largas y poco escalables. En su defecto se recomienda usar Route-Reflectors, tanto en sesiones iBGP como eBGP.*

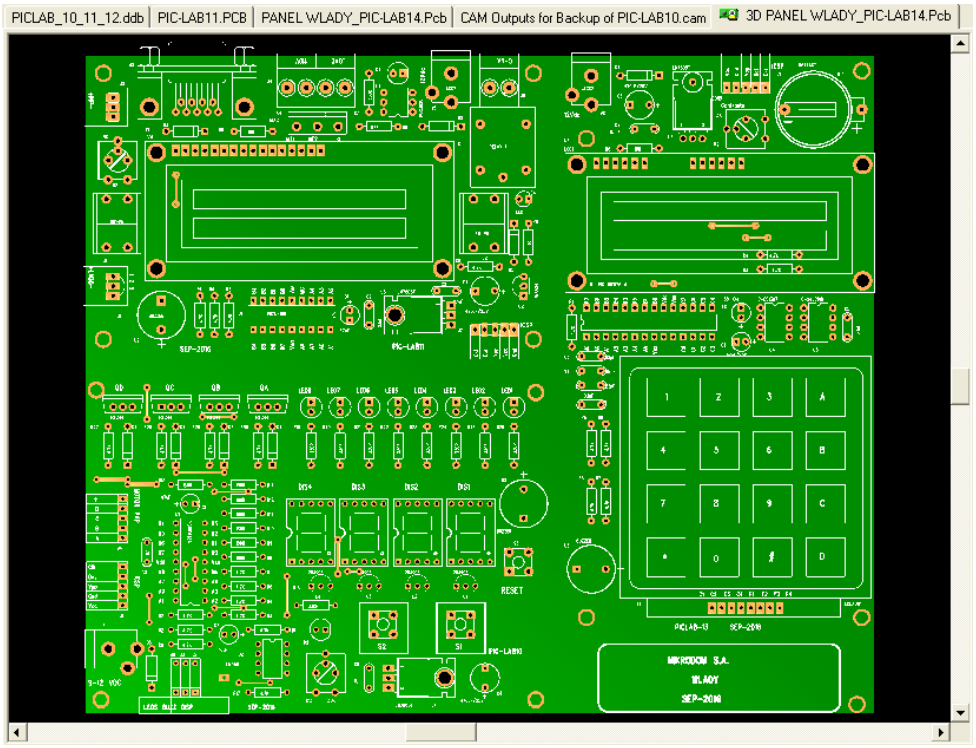
- *Se recomienda no publicar anuncios al ISP o Tier1 que contengan prefijos más específicos que /24. Esto ayuda que las tablas de enrutamiento sean más livianas y el tiempo de consolidación sea más rápido.*
- *La utilización de GLBP ayuda a conseguir compartición de carga en la red basado en el uso de diferente MAC Address y mayor capacidad de respuesta ya que pueden haber hasta cuatro equipos haciendo este trabajo. Esto hace que sea mejor que protocolos anteriormente usados como VRRP y HSRP.*
- *El uso de scripts en Cacti facilitan a personalizar las acciones que se pueden implementar en un sistema de monitoreo de redes.*
- *Si se configura una sesión OSPF es importante que las interfaces que unen los routers deben estar configuradas con los mismos timers, así como el mismo tipo de interfaces (Broadcast o NBMA).*

10. ANEXOS




MODEM
NO RESPONDE
PIC-LABII
PIC-LABIO
RESET
Cisco 2500 SERIES


IBM


PICLAB_10_11_12.ddb
PIC-LAB11.PCB
PANEL WLADY_PIC-LAB14.Pcb
CAM Outputs for Backup of PIC-LAB10.cam
3D PANEL WLADY_PIC-LAB14.Pcb
MIKROKOM S.A.
WLADY
SEP-2010