A Proposal for the Study, Analysis and Visualization of BGP Routes

Alexandra Ibarra Cuesta
ale@niclabs.cl

NIC Chile Research Labs
University of Chile

Abstract

Today's Internet is conformed by thousands of autonomous systems that exchange information using the BGP protocol, which has become the most important routing system since it allows Internet to carry out each of its tasks correctly. Given the above, it is highly important to identify routing problems with an easy to read and analyze mechanism. For this reason, this work proposes to design visualizations of the current state of the BGP routes from both a national and international view. It also proposes a subsequent study to find daily routing changes, and possible nodes that would cause routing failures after being removed from the network. Lastly, through these investigations it is intended to design BGP monitors, indicating where they should be located; as well as the mechanism for extracting the data necessary for them to work correctly.

1 Introducción

BGP (Border Gateway Protocol) nace por la necesidad de controlar la selección y propagación de rutas dentro de un Internet en expansión, transformándose en el sistema de enrutamiento más importante y complejo de todos los protocolos existentes puesto que permite el correcto funcionamiento de Internet. Por esta razón es importante la búsqueda de herramientas capaces de identificar problemas de enrutamiento. Asimismo, debido al gran número de rutas BGP existentes, sería útil facilitar este proceso de identificación mediante un sistema de monitoreo BGP que se encargue de recopilar y proveer información importante para luego llevar a cabo el análisis de la misma. Además, para comprender de mejor manera los datos recopilados por el sistema, así como también su análisis, es imprescindible utilizar un mecanismo de visualización mediante el cual sea posible observar tanto las rutas BGP existentes como la información relevante de los análisis realizados.

A partir de lo anterior, el trabajo propuesto se basa en diseñar una visualización de las rutas BGP que muestre el estado actual de las mismas. Esta representación debe ser capaz de mostrar toda la información requerida (rutas y las redes IP) en forma clara. Además, se realizará un estudio focalizado en dos puntos diferentes; por una parte está la identificación de cambios en las rutas BGP, para lo cual es necesario llevar a cabo un proceso comparativo del estado actual de la información con el anterior; el otro punto se basa en analizar el enrutamiento con el objetivo de obtener puntos críticos en el grafo, es decir, un nodo que al ser eliminado provoque, por ejemplo, un aislamiento completo de alguna red IP. Lo anterior conlleva al diseño de un sistema de monitoreo BGP, lo que implica establecer la cantidad y ubicación de puntos de control dentro de la red, así como también determinar el proceso de extracción de los datos y su posterior almacenamiento, procesamiento, análisis y visualización de los mismos.

2 Trabajo Relacionado

BGP ha sido un protocolo de constante estudio debido a la importancia que este representa para la comunicación entre redes. Trabajos anteriores han estudiado la vulnerabilidad de BGP, midiendo incluso el efecto que genera un ataque en el sistema de ruteo [ND04]; debido a esto es necesario identificar proble-

In: Proceedings of the IV School of Systems and Networks (SSN 2018), Valdivia, Chile, October 29-31, 2018. Published at http://ceur-ws.org

mas que puedan significar algún riesgo potencial para el envío y recepción de paquetes. Por esto, se han llevado a cabo diferentes investigaciones para diseñar monitores BGP. Estos trabajos proponen sistemas de recolección y análisis automatizado de la información de ruteo BGP, ayudando en la detección de comportamientos anormales en las rutas [Bor07], así como también alertando de cambios en las mismas [Yan+09], los cuales, según estudios realizados, pueden producir un efecto significativo en el flujo de información [TAR05].

Además, dadas las dificultades enfrentadas debido a la gran cantidad de datos obtenidos, es necesaria la búsqueda de un mecanismo de análisis simplificado. Respecto a esto último se han planteado o realizado varios mecanismos capaces de representar, visualmente, las rutas BGP tales como Link-Rank [LMZ04] [LMZ06], vizAS[1] (desarrollada por *APNIC*) y AS-Viewer [Hel11]. Junto a estas posibles formas de visualización para las rutas BGP se añaden los estudios realizados por *CAIDA* (Center for Applied Internet Data Analysis) que ha generado diferentes grafos de Internet[2]. Todas las investigaciones permiten generar una idea respecto al posible diseño a realizar para poder observar las rutas BGP.

3 Particularidad del trabajo propuesto

El sistema propuesto unirá dos trabajos independientes, es decir, el diseño de un sistema de monitoreo junto con visualizaciones de rutas BGP. Además incorporará nuevas funcionalidades, tal como la generación de grafos que entreguen una visibilidad tanto nacional como internacional de las rutas, lo cual permitirá analizar si estas son similares tanto desde dentro como desde fuera del país. Lo anterior corresponde a la diferencia principal con respecto a BGPmon dado que esta última no es georreferenciada. Este nuevo diseño tendrá también la particularidad de mostrar visualmente los cambios de ruteo identificados, lo cual, además de observar el tipo de modificación ocurrida, permitirá focalizar mejor el análisis de donde puede estar el problema o razón del cambio de ruteo. Por otra parte, este sistema se diferencia de los demás dado que busca identificar puntos claves que puedan conllevar, en un futuro, a un posible problema de flujo dentro de la red, siendo routers críticos en caso de ataques, fallas, entre otros.

4 Análisis Preliminar

Actualmente se cuenta con 3.485.877 datos reales que corresponden a rutas BGP, los cuales vienen almacenados en archivos que contienen diferentes tablas BGP. Estos datos fueron obtenidos por NIC Chile (administrador dominios punto CL) desde los distintos puntos de entrada de router de este. Es importante señalar que los datos utilizados corresponden a una muestra diaria obtenida a partir de la tabla BGP de solamente 7 Sistemas Autónomos diferentes (`AS6429`, `AS6471`, `AS7004`, `AS14259`, `AS18747`, `AS19338` y `AS27986`) debido a que son estos a los que tiene acceso NIC Chile.

En la Figura 1 se observa un ejemplo de la tabla BGP obtenida. Aquí se puede apreciar que presenta diferentes campos, donde los campos *Network* y *Path* son los únicos importantes para conformar una ruta, y por ende los que se utilizarán para trabajar. Cada una de las filas de esta tabla corresponde a una ruta BGP donde *Network* indica la IP de la red a la cual se desea llegar, mientras que *Path* es una serie de Sistemas Autónomos por los cuales se debe pasar para llegar a dicha IP; la unión de estos "puntos" conformará una ruta. En la Figura 2 se aprecia la ruta BGP obtenida a partir de la primera fila de la tabla de ruteo de la Figura 1. Cabe destacar que el nodo terminal del camino (IP Network) también corresponde a un Sistema Autónomo.

```
BGP table version is 0, local router ID is 200.1.123.20
Status codes: s suppressed, d damped, h history, * valid, > best,
              i - internal, r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop      Weight Path
*  1.0.0.0/24       200.73.16.185      0 18747 61522 7004 12956 13335 i
*  2.22.230.0/24    200.73.16.185      0 18747 61522 7004 20940 21342 i
*> 4.4.4.0/24       200.73.16.185      0 18747 19228 6471 27651 ?
*  8.23.24.0/23     200.73.16.185      0 18747 19411 19338 14259 6507 i
*  9.9.9.0/24       200.73.16.185      0 18747 19411 7004 61522 42 19281 i
*> 11.0.0.0/24      200.73.16.185      0 18747 19411 13424 ?
*  23.3.240.0/20    200.73.16.185      0 18747 61522 7004 20940 16625 i
```

Figura 1: Muestra un extracto de la tabla de ruteo del AS18747.

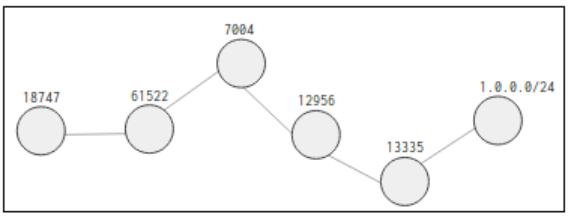

Figura 2: Muestra un ejemplo de ruta BGP, desde el AS18747 a la red IP 1.0.0.0/24, creada usando la librería D3 para JavaScript.

5 Trabajo a Desarrollar

Dado que se quiere realizar una investigación de las rutas BGP, y utilizando como base diferentes estudios

[1] vizAS: `https://blog.apnic.net/2015/09/09/visualise-your-countrys-bgp-network-with-vizas/`

[2] AS Core: `https://www.caida.org/publications/posters/#ascore`

que indican que utilizar una representación gráfica para llevar a cabo esta labor permite identificar de mejor manera errores de ruteo, se propone el desarrollo de visualizaciones que presenten, de manera correcta, los datos recopilados desde las tablas de ruteo de los diferentes routers a estudiar. Estas visualizaciones deben dar un panorama tanto nacional como internacional de las rutas BGP, respondiendo a las siguientes preguntas: ¿Cómo se ven las redes chilenas desde Chile?, ¿Cómo se ven las redes chilenas de manera internacional? y ¿Cómo se ven las redes internacionales desde una visión chilena? Para esto será necesario un estudio previo respecto a cada una de las direcciones IP obtenidas con el objetivo de identificar cuales de estas corresponden a IPs nacionales y cuales a internacionales.

En base al sistema diseñado, se llevará a cabo un estudio de estas para encontrar cambios generados en las rutas BGP, para esto se debe implementar una forma de poder recuperar diariamente la información de ruteo para que, tras su procesamiento, se logre obtener automáticamente su representación y, además, los cambios de enrutamiento con respecto a la información antigua, lo cual implica desde la ausencia de un Sistema Autónomo previo hasta el cambio como tal de una ruta (utilizar otros Sistemas Autónomos). Además, se realizará un análisis del grafo generado para lograr identificar nodos críticos, es decir, routers que al ser desconectados o presentar alguna falla generen, por ejemplo, que redes IP no sean alcanzables por ninguna otra ruta provocando un aislamiento completo de dicha red.

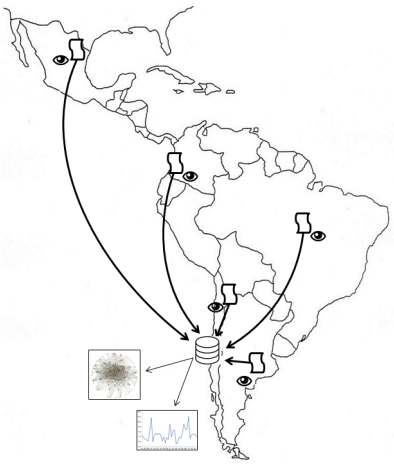

Figura 3: Esquema del sistema de monitoreo. Cada punto de control se representa por un "ojo".

Finalmente, se diseñará un sistema de monitoreo el cual une cada una de las características anteriores, es decir, se dispondrán puntos de control encargados de recopilar, diariamente, información de las tablas de ruteo de diferentes routers para luego, enviar todos los datos obtenidos a una base de datos "global" de manera automática; esto dará paso al procesamiento y análisis de estos datos y su posterior visualización (ver Figura 3).

6 Metodología

La metodología de trabajo se divide en diferentes etapas de desarrollo.

6.1 Manejo de la tabla de ruteo

Se deben establecer los campos de extracción de las tablas de ruteo, tales que estos permitan definir una *ruta BGP*. Debido a lo anterior, se deben realizar diferentes parser que se encarguen de extraer la información y llevarla, finalmente, al formato que será utilizado para crear la visualización.

En cuanto a este punto es posible mencionar que ya se establecieron los parámetros de extracción, tal y como se mencionó anteriormente, siendo estos campos: *Network* y *Path*. Además, se han realizado diferentes programas en Python, encargados de la sustracción de dichos datos y su transformación al formato utilizado actualmente, el cual consiste en un json donde cada nodo presenta la siguiente estructura:

```
{"node": {
  "id": id_node,
  "group": group_node,
  "label": label_node
}}
```

Donde *id_node* corresponde al AS o a la red, por ejemplo, si el nodo representa al AS 7004, entonces *id_node* tendrá el valor 7004; *group_node* identificará si el nodo en cuestión corresponde a un AS, en cuyo caso *group_node* será 1, o si es una IP, por lo que tendrá el valor 2; mientras que *label_node* será un identificador interno de cada nodo dentro de su grupo respectivo.

6.2 Diseño de visualización

Se analizarán diferentes tipos de visualizaciones para encontrar la que mejor se adapte a los objetivos planteados. Para llevar a cabo este proceso se utilizará *JavaScript*, junto con la librería gráfica *D3*.

Actualmente se cuenta con un modelo básico de visualización, el cual nació de las representaciones ya realizadas en trabajos previos, como por ejemplo CAIDA. Este modelo se caracteriza por ser un grafo circular, donde su frontera se conforma por los nodos correspondientes a las IPs, mientras que los nodos internos son los sistemas autónomos utilizados en el ruteo de información.

Cabe destacar que debido a la gran cantidad de información, el grafo diseñado contiene agrupación de

IPs según su ruteo, es decir, se unieron en un solo nodo aquellas redes que presentaban el mismo camino de sistemas autónomos, permitiendo disminuir en gran medida el exceso de información visual, clarificando las rutas existentes.

En la Figura 4 se encuentra la representación desarrollada hasta ahora la cual se debe seguir modificando, dado que se debe mejorar el posicionamiento y distribución actual de los nodos, puesto que varios de estos se ubican alejados de sus puntos de conexión inmediatos, generando aristas de gran longitud, lo que provoca que la visualización sea más compleja y difícil de entender.

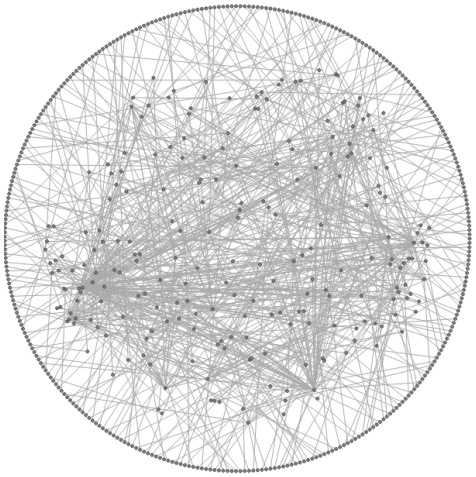

Figura 4: Prototipo de visualización desarrollada actualmente.

Además, se seguirá analizando la forma de agrupar los datos de manera tal que disminuya la congestión de información, por ejemplo por prefijos de IPs; así como también agregar diferentes características al modelo, que permitan que la información sea más fácil de analizar por un observador externo, por ejemplo, añadir interactividad, gama de colores, transparencia, entre otros, para resaltar zonas relevantes. Esta medida es vital debido a la gran cantidad de datos que deben contener cada uno de los gráficos a generar, permitiendo focalizar la atención del observador en ciertos puntos de interés según el sistema de monitoreo, facilitando un seguimiento y estudio más focalizado de un posible problema de ruteo.

6.3 Identificación de IPs

Es necesario identificar la localización geográfica tanto de las IPs como de los sistemas autónomos, debido a que se deben realizar visualizaciones de carácter tanto nacional como internacional de las rutas BGP. Para esto se utilizarán trabajos y/o herramientas ya existentes tales como: MaxMind[3], LacNic[4], entre otros.

6.4 Trabajo futuro

A largo plazo se deben desarrollar las características principales del sistema de monitoreo, es decir, analizar y desarrollar otros tipos de representaciones gráficas, y establecer cómo desarrollar las visualizaciones específicas, eligiendo la representación que mejor se adapte para solucionar el problema. Además, se deben implementar programas de análisis de rutas para identificar cambios de ruteo y puntos críticos en la red. Finalmente, se debe determinar el proceso de extracción de los datos reales utilizados por el sistema de monitoreo, de manera que sea automatizado, y su posterior procesamiento y visualización.

Referencias

[Bor07] Gunnar Bornemann. "Data Analysis and Design of a BGP Monitoring and Alarm System". En: *Diploma Thesis in Computer Science, Technische Universität München* (mar. de 2007).

[Hel11] Mathias Helminger. "Interactive visualization of global routing dynamics". En: *Bachelor Thesis in Informatics, Technische Universität München* (jun. de 2011).

[LMZ04] Mohit Lad, Dan Massey y Lixia Zhang. "Link-Rank: A Graphical Tool for Capturing BGP Routing Dynamics". En: *Network Operations and Management Symposium (NOMS)* (abr. de 2004).

[LMZ06] Mohit Lad, Dan Massey y Lixia Zhang. "Visualizing Internet Routing Changes". En: *IEEE Transactions on Visualization and Computer Graphics* (nov. de 2006).

[ND04] Ola Nordström y Constantinos Dovrolis. "Beware of BGP Attacks". En: *SIGCOMM Comput. Commun. Rev.* 34.2 (abr. de 2004), págs. 1-8.

[TAR05] Renata Teixeira, Sharad Agarwal y Jennifer Rexford. "BGP Routing Changes: Merging Views from Two ISPs". En: *SIGCOMM Comput. Commun. Rev.* 35.5 (oct. de 2005), págs. 79-82.

[Yan+09] He Yan y col. "BGPmon: A Real-Time, Scalable, Extensible Monitoring System". En: *2009 Cybersecurity Applications Technology Conference for Homeland Security* (2009), págs. 212-223.

[3] https://www.maxmind.com/en/home
[4] https://rdap-web.lacnic.net/