UNIVERSIDAD DE CHILE
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

SANIDAD DE RUTAS CHILENAS EN INTERNET

MEMORIA PARA OPTAR AL TÍTULO DE INGENIERO CIVIL EN COMPUTACIÓN

PABLO IGNACIO SEPÚLVEDA ROJAS

PROFESOR GUÍA:
TOMÁS BARROS ARANCIBIA

MIEMBROS DE LA COMISIÓN:
JOSÉ MIGUEL PIQUER GARDNER
NELSON ANTRANIG BALOIAN TATARYAN

SANTIAGO DE CHILE
ABRIL 2010

Resumen

Internet es una red de redes; para poder comunicarse, se debe encontrar un camino entre el emisor y el receptor. El protocolo más usado para encontrar caminos entre redes distantes es Border Gateway Protocol (BGP). Este protocolo se basa en la confianza, por lo que es vulnerable a ataques y a errores de configuración, además, estos errores se propagan rápidamente, pudiendo afectar una parte considerable de Internet. Por esto se hace necesario contar con herramientas que detecten estos problemas.

Cada red se dice *visible* desde algún punto, si desde ese punto se puede enviar información hacia esa red. El ideal de internet, es que todas las redes sean visibles desde todos los puntos, pero por los problemas antes mencionados, esto no siempre se cumple. En este trabajo se estudió el porcentaje de visibilidad de las redes chilenas, agrupadas por empresa.

Para esto se creó una herramienta dividida en tres partes: recolección de datos, procesamiento y visualización de los datos. La visualización se realiza vía web, y cuenta con gráficos generados dinámicamente, para ayudar a una mejor comprensión de los datos.

Los resultados mostraron que Chile tiene una alta visibilidad, cercana al 100 % en IPv4, mientras que en IPv6, se mantiene cercana al 82 %. Así mismo, la cantidad de redes usadas difiere notablemente entre ambas versiones, se usan 315 redes chilenas IPv4 y sólo 13 de IPv6.

Se concluye que las redes chilenas tienen una configuración adecuada, que les permite ser alcanzables desde todos los puntos estudiados. Además estas configuraciones son bastante estables. Se constató también que si bien IPv6 está aún muy por debajo de IPv4 en penetración, esta ha ido aumentando.

Agradecimientos

Agradezco a mis padres Alejandro e Irene por su apoyo incondicional durante toda mi vida.

A NicLabs por el apoyo logístico y por confiar en mí, especialmente a Tomás por la confianza depositada y a Víctor por sus ayuda en la organización de esta memoria.

Agradezco también a Alejandra por su compañía y su esfuerzo por entenderme a pesar de nuestras diferencias.

Gracias a toda la gente que leyó y ayudó a corregir mi memoria: Alejandra, Alejandro, Carlos, Jo, Tomás y Víctor.

Índice General

Capítulo 1

Introducción

Internet, llamada la red de redes, es una red global descentralizada, compuesta de muchas redes más pequeñas interconectadas. Una red es una agrupación de computadores o dispositivos, estas redes se agrupan a su vez en conjuntos más grandes, Internet es una agrupación mayor de estas redes. Una red que está bajo el control de una sola organización, se llama Sistema Autónomo (conocido como AS, de su sigla en inglés Autonomous System) [23]. Internet es la unión de los distintos Sistemas Autónomos existentes en el mundo.

Como no todos los nodos están conectados entre sí, para poder comunicar dos equipos, se debe encontrar caminos que conecten ambos puntos. Este proceso denomina routing. Cuando ocurre dentro de un Sistema Autónomo es llamado routing intra-dominio y el routing entre distintos Sistemas Autónomos se conoce como routing inter-dominios. El routing inter-dominio usado en Internet es el Border Gateway Protocol [24] (BGP). BGP es un protocolo relativamente simple, recibe rutas desde sus vecinos y las compara con las que ya tenía, si hay alguna ruta mejor, la reemplaza y la anuncia a sus propios vecinos. Esto permite flexibilidad al momento de decidir que es mejor, configurando parámetros de acuerdo a las propias conveniencias. Es esta simplicidad lo que le ha permitido tener el rol principal en la Internet global, sin embargo históricamente ha tenido muy pocas garantías de seguridad, pues en su diseño original no fue considerado [26]. Cada Sistema Autónomo confía en sus vecinos. En este sentido, es fácil mentir y hacer creer a un router que se tiene un mejor camino hacia cierto destino, con el propósito de denegar un servicio, o espiar los datos que se envíen. La pérdida de accesibilidad en Internet, puede deberse a errores humanos, por ejemplo: mala

configuración de un router, o a actividades maliciosas.

Un ejemplo de una configuración BGP con tres Sistemas Autónomos se muestra en la figura 1.1, el Sistema Autónomo 100 con un router, el Sistema Autónomo 200 con tres routers y el Sistema Autónomo 300 con un router. Dentro del Sistema Autónomo 200, los routers se comunican usando IBGP, (Internal BGP) y los routers de borde (RTB y RTC) utilizan EBGP (External BGP) para comunicarse con los routers pertenecientes a los otros Sistemas Autónomos.

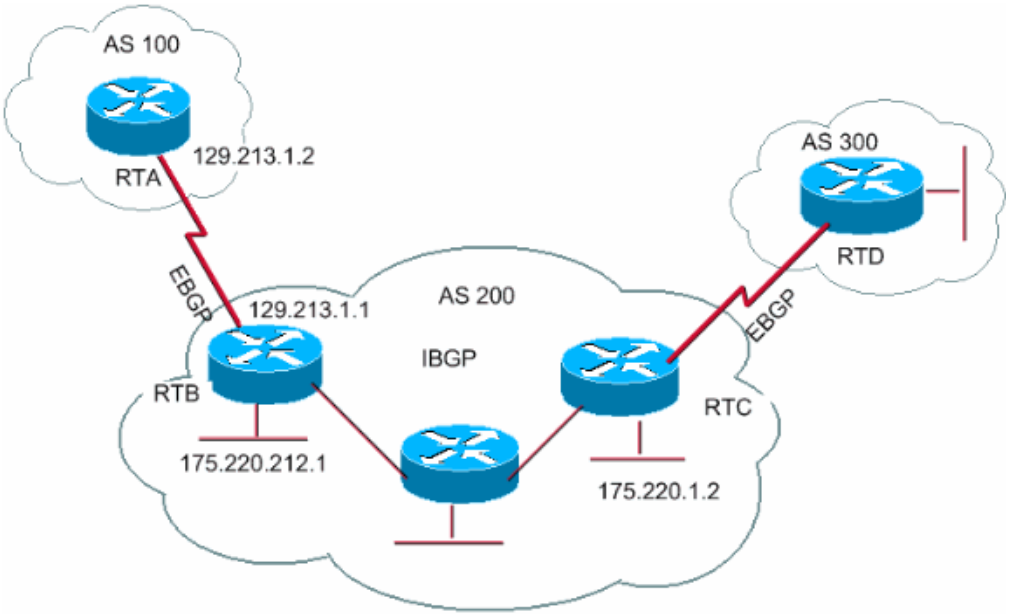

Figura 1.1: Gráfico de un sistema de interacción BGP. Fuente: Cisco.

Debido a la falta de seguridad (o al exceso de confianza) y al aspecto inter-dominio de BGP, incluso pequeñas fallas dentro de un Sistema Autónomo pueden, en ocasiones, propagarse ampliamente al resto de Internet, causando un daño maviso. [26]

Una de estas fallas, ocurrió en abril de 1997, cuando un router mal configurado de un pequeño proveedor de acceso a Internet (Internet Service Provider, ISP) insertó información errónea en Internet global, diciendo que tenía una ruta óptima a todos los destinos [26]. Como no hay una forma de validar los anuncios de ruta, la mayor parte del tráfico de Internet fue redirigida a este ISP, lo que dejó sin acceso a Internet a una porción relevante del total de usuarios, por casi dos horas.

Otro problema más reciente fue el llamado Hijack (secuestro) de Youtube [4]. El 24 de

febrero de 2008, Pakistán Telecom comenzó a avisar que cierta parte de la red de Youtube le pertenecía. Esto ocasionó que cerca de dos tercios de los usuarios de Internet que querían acceder a esa parte de la red, fueran redirigidos hacia Pakistán Telecom, dejándolos sin poder ver sus videos. Este "ataque" fue hecho intencionalmente, ya que el gobierno había ordenado bloquear el acceso a Youtube, pero a los usuarios de su país solamente. Gracias a la rápida reacción del equipo de Youtube, y a la cooperación de otros proveedores,el problema duró sólo un par de horas.

El 2008, en la conferencia de Hackers, o de seguridad computacional, Defcon [9], dos investigadores mostraron como es posible hacer un ataque de "hombre en el medio[1]" para BGP [22]. Es decir es posible interceptar el tráfico hacia ciertos destinos, observarlo e incluso modificarlo y luego reenviarlo hacia el destino, todo esto simplemente por el modelo de confianza de BGP.

Problemas como los mencionados, motivaron la aparición de herramientas para revisar que se esté ruteando correctamente, es decir que no se esté perpetrando alguno de estos ataques, o algún ataque de otro tipo, pues estos podrían ser detectados al observar el AS Path, es decir el camino de un punto a otro.

BGP ha sido el protocolo de routing en Internet por más de 10 años, durante los cuales numerosos problemas han sido descubiertos. Los administradores de cada red pueden proteger sus redes de la mayor parte de estos problemas usando autentificación, y otras buenas prácticas. Sin embargo no es posible verificar eficientemente el contenido de un mensaje BGP [5], por defecto un router cree la información que recibe.

Todos estos problemas de Internet, ocasionan demoras en el tráfico e incluso pérdida de alcance de algunos destinos. En este estudio, se define la *visibilidad* como la propiedad de que un destino sea alcanzable desde el resto del mundo. En el caso Pakistán-youtube, por ejemplo, el destino (youtube) dejó de ser efectivamente alcanzable, y no sólo desde Pakistán, sino que también desde muchas otras partes del mundo. En este trabajo se estudiará hasta qué punto son efectivamente visibles las redes chilenas desde el mundo.

[1] man in the middle

El protocolo de comunicación usado actualmente es Internet Protocol (IP), ya sea en su cuarta o sexta versión (IPv4 [19] e IPv6 [8]). Cada computador debe tener un número IP único que lo identifique dentro de Internet. Los números IP son delegados a organizaciones y a los ISP (por ejemplo: Telmex Chile, Telefónica) para que éstos puedan administrarlos dentro de su red interna.

ICANN (Internet Corporation for Assigned Names and Numbers) es la organización responsable de la asignación de direcciones IP a nivel mundial, a su vez, ICANN delega esta responsabilidad a otras organizaciones que agrupan países de acuerdo a su ubicación geográfica. En el caso de Chile, el registro de direcciones para la región está a cargo de Latin American and Caribbean Internet Addresses Registry (LACNIC). LACNIC tiene un registro público de IPs y Sistemas Autónomos asignados, indicando el país. Desde allí se pueden obtener las IPs que corresponden a la zona chilena; para de esta forma hacer el estudio centrado específicamente en nuestro país. Determinar la localización geográfica a partir de la IP no es trivial para el caso general, ver el trabajo de CAIDA [14].

Esta memoria, pretende obtener información acerca de la visibilidad actual de Internet en Chile, es decir la cantidad de IPs visibles desde distintos puntos del mundo. Para esto, existen servidores llamados "looking glasses" que entregan información de visibilidad de una IP, estos servidores están ubicados alrededor del mundo, pero sólo permiten consultar por una IP, no por un conjunto con un criterio distinto como serían las IPs chilenas.

1.1. Motivación

Quisiéramos saber qué porcentaje de todas las IPs de Chile son visibles desde el mundo, como una medida de la visibilidad de nuestra red; es decir hacer el estudio para todas las IPs de Chile, con la finalidad de tener datos agregados a nivel país, que permitirían conocer la realidad chilena en esta temática.

En esta misma línea, es relevante saber si el problema de la visibilidad es, por ejemplo, responsabilidad de algún ISP en particular, es decir tratar de aislar lo mejor posible el problema para notificar a los involucrados de modo que el problema pueda ser estudiado y en lo

posible solucionado por los responsables específicos.

La memoria pretende investigar la visibilidad y el crecimiento de Internet en Chile, qué IPs son compradas en Chile y cuáles son efectivamente visibles. De este modo se pretende obtener no solo una fotografía de Internet, sino que además poder ir componiendo estas fotografías en el tiempo para ver su evolución temporal. Los datos que se obtengan a partir de este trabajo, pueden ser usados, entre otros para ver como migra Chile realmente desde IPv4 hacia IPv6.

1.2. Objetivo general

El objetivo general es medir la visibilidad de las redes chilenas, así como su variabilidad en el tiempo, tanto de IPv4 como IPv6.

1.3. Ojetivos específicos

- Crear una métrica para medir la visibilidad de las redes chilenas.
- Crear (o adaptar) una herramienta que permita medir la visibilidad de las redes chilenas.
- Realizar esta medición de forma constante, y publicar la información para el público.
- Medir crecimiento de Internet en Chile (IPs compradas y visibles)
- Separar en IPv4 e IPv6, para hacer una comparación entre éstas dos.

1.4. Metodología

La metodología que se siguió en el estudio fue la siguiente:

1. Se revisaron protocolos para conectarse a los "looking glasses" existentes, de manera de crear (o adaptar) un cliente que pruebe con las IPs pertenecientes a Chile, así como con los Sistemas Autónomos chilenos.

2. En una primera etapa, se investigaron formas de obtener los datos, ya sea conectándose directamente o mediante el uso de datos ya recolectados.

3. En una segunda etapa se realizaron pruebas para todas las redes chilenas.

4. Luego se ordenaron las redes jerárquicamente, para poder obtener datos con sentido, es decir, saber si se anuncia la red, o una parte de ella, porcentaje de visibilidad, un mapa de visibilidad que contenga: punto de referencia, red observada.

5. Se construyó un programa para recolectar y procesar los datos.

6. Se recolectaron y procesaron datos desde el 17 de noviembre, hasta febrero al menos una vez por semana.

1.5. Organización de la memoria

La estructura de esta memoria, por capítulos, es la siguiente:

1. Capítulo 2, Contexto, define conceptos necesarios para la comprensión de la memoria, además de hacer la revisión de los trabajos relacionados que se han desarrollado en el mundo.

2. Capitulo 3, Procedimiento, muestra el procedimiento teórico realizado para realizar la medición, desde la definición de las métricas hasta los pasos a seguir.

3. Capítulo 4, Implementación, detalla el desarrollo específico de software que fue necesario para realizar el estudio.

4. Capítulo 5, Resultados, expone los resultados obtenidos al usar la herramienta desarrollada.

5. Capítulo 6, Conclusiones, condensa los logros obtenidos, explicitando también como se podría mejorar el sistema.

Capítulo 2

Contexto

En este capítulo se explica como funciona Internet, cómo es posible que dos computadores en casi cualquier lugar del mundo sean capaces de comunicarse. Esto no al nivel de la existencia del cable, o satélite que los comunica, sino que al nivel de cómo distinguir de entre todos los computadores interconectados, a cual se le debe entregar el mensaje. Esta explicación no pretende ser completa, pero debe ser suficiente para entender el resto de la memoria. En una segunda parte se revisan las investigaciones desarrolladas para medir la calidad de Internet en el mundo, así como también las herramientas existentes con este mismo fin.

2.1. Breve introducción a Internet routing

Internet es conocida como una red de redes. Una red es un conjunto de equipos (computadores), entonces Internet sería un conjunto de conjuntos de computadores.

Routing es el proceso de elegir caminos en una red para enviar el tráfico. Los equipos que realizan esta función son los denominados routers.

La información del camino se almacena en una tabla (de rutas), que puede ser tanto estática, como dinámica. En la tabla de ruta se debe almacenar el siguiente salto, es decir a quién se le debe enviar la información. Los computadores que no son routers, generalmente sólo tienen una ruta, llamada ruta por defecto, que indica que cualquier paquete que deseen

enviar, se debe mandar a su router, el que se encargará de hacer llegar la información a destino.

Las tablas de rutas estáticas son rápidas, pero requieren mantenimiento continuo, editarlas manualmente al ocurrir algún cambio en la red. Las tablas dinámicas se crean usando distintos protocolos, dependiendo de si los equipos son parte de la misma red, de un mismo Sistema Autónomo o si están en Sistemas Autónomos distintos.

Un protocolo de red es un conjunto de procedimientos y lenguajes que un router usa para comunicar la información de routing a otros routers, es decir un algoritmo y una forma de comunicarse. La ventaja de utilizar algoritmos es la capacidad de adaptarse a una topología cambiante, notificando a otros routers del cambio o fallo acontecido, dinámicamente [7].

Para la comunicación entre dos redes, pero dentro de un mismo Sistema Autónomo, se puede usar Open Shortest Path First (OSPF), que encuentra el camino más corto entre estas dos redes, utilizando una adaptación del algoritmo de Dijkstra para buscar el camino mínimo en un grafo. La distancia es medida como la cantidad de routers por los que hay que pasar para llegar al destino. El router que tiene la red, debe avisarle a los otros que él la tiene, esto se denomina anunciar la red, así cuando se dice que una red fue anunciada, quiere decir que un router le avisó a otros que él poseía tal red.

Finalmente, para comunicarse entre distintos Sistemas Autónomos, se utiliza Border Gateway Protocol (BGP), que decide un camino basándose no sólo en el camino (AS Path) más corto, que se mide cmlo la cantidad de Sistemas Autónomos por los que hay que pasar, sino que también se fija en ciertas reglas y políticas de red. En este trabajo sólo nos concentraremos en BGP, puesto que es el protocolo utilizado para difundir las redes chilenas por el mundo.

2.2. BGP

La versión del protocolo BGP actualmente en uso (v4) es la del RFC 4271 [24]. A diferencia de los protocolos de routing interno, como RIP u OSPF, donde existe un único

parámetro para elegir el mejor camino, BGP utiliza una serie de atributos para elegir el mejor camino a cada prefijo, el que no necesariamente será el camino más corto.

BGP organiza la red en Sistemas Autónomos (AS), los que corresponden a una entidad, ya sea un ISP, Universidad, empresa, etc. Normalmente un AS agrupa a muchas

Dos routers son llamados vecinos o pares si es que comparten una sesión BGP. La sesión BGP comienza con un handshaking, donde los routers negocian opciones, tales como extension del del protocolo o soporte IPv4 y/o IPv6.

Cada AS se puede clasificar dentro de tres tipos:

Stub AS o Sistema Autónomo Hoja, aquél que sólo se conecta con un único AS (su proveedor).

Multihomed AS o Sistema Autónomo Multiconectado, que se conecta a más de un Sistema autónomo, pero no permite tráfico a través de él.

Transit AS o Sistema Autónomo de tránsito, que permite que el tráfico pase a través de él.

Una vez establecida la sesión, los routers intercambian información sobre las redes que conocen mediante updates (actualizaciones), éstas pueden ser anuncios o retiros (withdrawals), es decir un nuevo camino a alguna red o el que un camino deje de ser utilizable. Un anuncio contiene la red de destino, el AS Path, el próximo salto, es decir a quien debe enviársele el paquete y otros atributos usados por extensiones específicas.

Cada router almacena una tabla con las redes que puede acceder, y otra con las rutas que le comunica cada vecino. Luego elige cuales de estas rutas, "promover" a su tabla de ruta, es decir decide usar alguna de las rutas que le comunicó su vecino. Para elegir una ruta, ve si el siguiente salto es alcanzable, es decir está en su tabla de rutas, además chequea su preferencia local dependiendo del tipo de relación que se tenga con el vecino (si es proveedor, par o cliente).

2.2.1. Algoritmo de selección de rutas

En la práctica cada compañía fabricante de routers ha decidido procedimientos para elegir las rutas, estos procedimientos toman en cuenta parámetros extras o métricas propias de cada implementación. El algoritmo general es el siguiente:

1. Aplicar políticas configuradas por el usuario para ajustar variables (variar el Local Preference basado en el atributo Comunidad, por ejemplo)
2. Seleccionar la ruta con el más alto valor de Local Preference
3. Si hay más de una, seleccionar la ruta con el AS Path más corto
4. Si hay más de una, seleccionar la ruta con el atributo Origin menor.
5. Si hay más de una, seleccionar la ruta con el valor MED más alto si las rutas fueron recibidas desde el mismo Sistema Autónomo o si el router está configurado para comparar MEDs
6. Si hay más de una, seleccionar la ruta aprendida por EBGP
7. Si hay más de una, seleccionar la ruta tal que su NEXT HOP tenga el mejor costo
8. Si hay más de una, seleccionar la ruta que haya sido anunciada por un BGP con mayor identificador
9. Seleccionar la ruta recibida por el vecino con menor dirección.

2.2.2. Propagación de rutas

Cuando un router BGP recibe una nueva ruta a través de un mensaje de actualización, ejecuta el siguiente procedimiento:

1. Verifica si existe algún filtro de entrada en la sesión, si la ruta no es permitida, se ignora y el proceso termina.

2. Inserta la ruta en la tabla BGP

3. Compara la ruta con otras rutas al mismo prefijo destino de la tabla BGP y ejecuta el algoritmo de selección de rutas. Si la nueva ruta no es considerada como la mejor, el proceso se detiene.

4. Toma la nueva ruta como la mejor y la incluye en su tabla de rutas (general, no sólo BGP). La anterior mejor ruta es eliminada.

5. Propaga la nueva mejor ruta a sus vecinos BGP en otros Sistemas Autónomos, si sus filtros lo permiten, agregando su propio Número (ASN) al AS Path.

6. Propaga la nueva mejor ruta a sus vecinos dentro de su Sistema Autónomo, a menos que la ruta haya sido aprendida dentro del mismo Sistema Autónomo (IGP).

Cada Autonomous System puede ajustar sus parámetros para elegir tal o cual ruta. Si un Sistema Autónomo prefiere que no lo elijan como ruta, puede utilizar AS prepending, que consiste en agregar su ASN varias veces al AS Path, de esta forma alarga artificialmente el camino, disminuyendo las probabilidades de que que otros Sistemas Autónomos lo elijan como mejor ruta.

En la figura 2.1 se tiene un esquema muy simplificado de Internet. Cada router representa un Autonomous System. Así, en este ejemplo, los vecinos serían los del cuadro: 2.1.

Sistema Autónomo	**Vecinos**
2324	664
664	2324, 23
23	664,112,6012
112	23
6012	23, 3024
3024	6012

Cuadro 2.1: Autonomous Systems vecinos en el ejemplo de la fig: 2.1

Y los AS Path que tendrían para la red 200.24.0.0/16 serían los del cuadro: 2.2. Cada uno tiene en su tabla de ruta entradas similares para cada una de las redes que conoce.

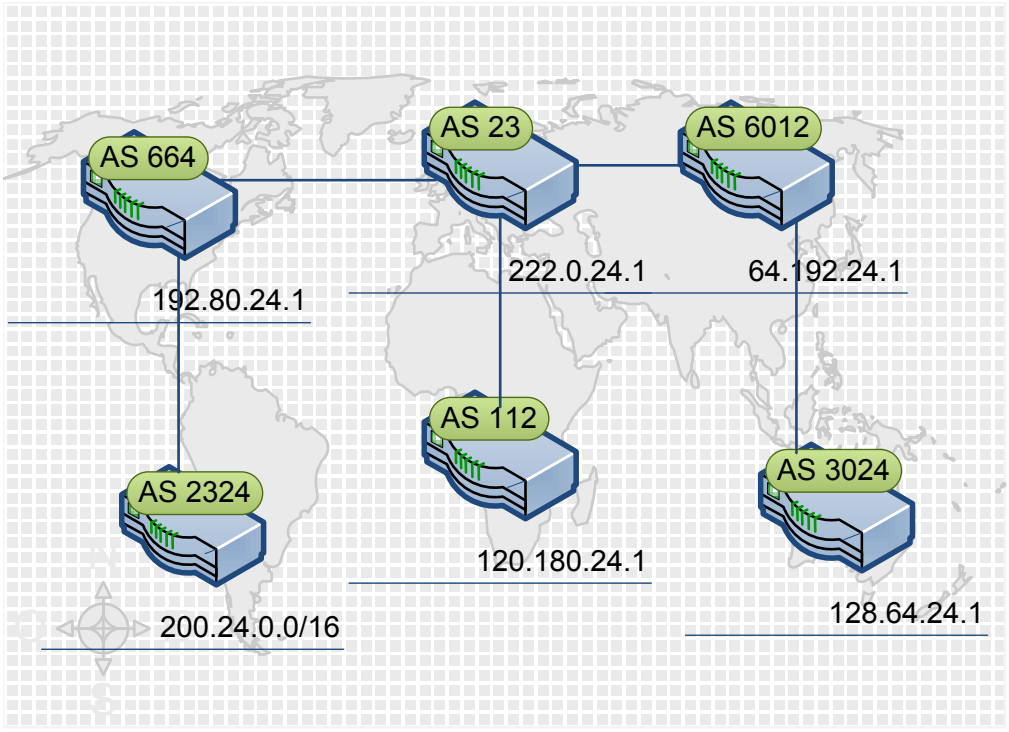

Figura 2.1: Autonomous Systems

En este ejemplo, desde el router del Sistema Autónomo 112, la mejor forma de llegar a la red 200.24.0.0/16, es pasando por el Sistema Autónomo 23, luego por el Sistema Autónomo 664, y luego por el Sistema Autónomo 2324. Además, sabe que debe enviar todo el tráfico destinado a esa red, al router 222.0.24.1, pues éste se encargará de hacer llegar el tráfico a la red 200.24.0.0/16.

Sistema Autónomo	**AS Path**	**Next hop**
664	{2324}	200.24.0.1
23	{664,2324}	192.80.24.1
112	{23,664,2324}	222.0.24.1
6012	{23,664,2324}	222.0.24.1
3024	{6012,23,664,2324}	64.192.24.1

Cuadro 2.2: AS Path de cada Autonomous System para la red 200.24.0.0/16, según el ejemplo de la fig: 2.1

2.3. Trabajo relacionado

El primer estudio completo de la sanidad de Internet fue hecho en 1997 [15]. Allí se observó por nueve meses el tráfico a través de 5 puntos de intercambio de mensajes BGP. Sus principales descubrimientos fueron la gran cantidad de actualizaciones que se realizaban, la mayor parte patológica, es decir información errónea o redundante, es decir que repetía información ya conocida. Casi diez años después, se realizó un estudio similar, [18] con datos desde agosto 2005 a enero 2006, mostrando una clara mejora en la salud de BGP, los mensajes patológicos disminuyeron notablemente su presencia, quedando de estos, mayoritariamente los anuncios redundantes.

En estos estudios no se mide exactamente lo que se pretende medir en esta memoria, sin embargo, se mide la sanidad de la red, que debería estar directamente relacionada. Es decir a mayor sanidad, debería haber mayor visibilidad, o una mejor conectividad, pues debería haber menos errores.

Además de esos estudios, existen iniciativas para almacenar la información de routing y dejar esta información públicamente disponible. Entre ellas están los archivos mantenidos por el Proyecto Vista de Rutas de la Universidad de Oregon (University of Oregon's Route Views Project) [28], los archivos RIPE [25] y el Monitor BGP del MIT [11], de aquí en adelante estos servidores serán conocidos como servidores recolectores, o simplemente recolectores.

Los recolectores, almacenan la información tal como se originó, es decir los mensajes de actualización, por lo que, para obtener información o estadísticas de ellos es necesario crear herramientas que hagan uso de esta información para mostrar distintas aristas según lo que se pretenda analizar con el estudio.

Iniciativas que usan los datos recolectados, son BGPMon [27] y Cyclops [20], los que además de permitir hacer consultas, generan alertas ante cambios, con la idea de detectar redireccionamientos maliciosos, o por errores de configuración. Al registrarse, permite monitorear ya sea uno o múltiples Sistema Autónomo, y configurar las alertas que se desean recibir. Además BGPMon, permite visualizar gráficamente la cantidad de IPs ya sea IPv4

o IPv6 por país. Por otro lado Cyclops mantiene datos de las relaciones entre los Sistemas Autónomos, es decir quién es proveedor de quién, Sistemas Autónomos hermanos, etc.

2.3.1. Cyclops

Cyclops utiliza información de RouteViews, RIPE-RIS, Abilene [1], Packet Clearing House [21] y Bgpmon para proveer una herramienta que permite comparar el comportamiento esperado del comportamiento observado. La herramienta permite seleccionar uno o más Sistemas Autónomos que se deseen supervisar, definiendo los vecinos y las relaciones con ellos y también las redes que se anuncian desde cada uno de los Sistemas Autónomos. El sistema puede deducir estos elementos a partir de los datos observados, pero permite también introducir los datos manualmente. Luego de la configuración inicial, la herramienta generará alertas cada vez que una de las redes sea anunciada por algún otro Sistema Autónomo, que se cree alguna nueva interconección entre Sistema Autónomo, que haya algún cambio en los caminos alrededor de los Sistemas Autónomos supervisados o que alguno de los Sistemas Autónomos anuncie otra red distinta. Todas estas alertas sirven para detectar casos de denegación de servicio, o de espionaje, además de detectar las configuraciones erróneas en los Sistemas Autónomos.

Herramientas como Cyclops o BGPMon, son muy útiles para detectar errores de routing hacia las redes, pero no tienen el análisis histórico ni tampoco se centran específicamente en Chile, por lo que no es directo obtener información respecto al país.

2.3.2. Looking-glasses

Aparte de los recolectores, existen actualmente servidores "looking glasses," que permiten obtener información de routing, desde ese punto hasta cualquier otro punto [17], ingresando la IP del destino, así se puede preguntar por cierta red, para hacer consultas con respecto a más redes (como en este caso para todas las redes chilenas), habría que repetir la consulta, ya sea manualmente o con un programa que lo haga de forma automática.

Cooperative Association for Internet Data Analysis (CAIDA), es una asociación que provee herramientas y análisis, promoviendo el mantenimiento de una infraestructura de Internet escalable y robusta. Dentro de esos análisis CAIDA ha hecho estudios en el área de la visibilidad [14], para la zona Asia-Pacífico, en esta investigación, se incluyó Chile, pero sólo con 28 destinos en el país. En este estudio se midió cómo se llegaba desde cierto punto a muchos destinos. Un estudio similar es el que se pretende realizar en esta memoria, pero centrado exclusivamente en Chile como destino, y con una gran cantidad de lugares de origen.

También se han realizado estudios con el fin de conocer las relaciones entre los Sistemas Autónomos. Uno de estos fue el realizado por Gao el 2001 [12], donde se muestra un método para inferir las relaciones a partir de las tablas de ruta públicas, con gran éxito, un 99,1 % de las relaciones deducidas eran correctas. Sin embargo, en un estudio posterior, Dimitropoulos, el 2006 [10], concluye que hay un porcentaje significativo de las interconexiones que no aparecen en las tablas de ruta, pues existe otra ruta mejor (por ejemplo las relaciones que no aparecen podrían corresponder a rutas de respaldo). Por esto, para este trabajo se ha decidido usar información existente con respecto a las conexiones entre Sistemas Autónomos, específicamente la información que maneja Cyclops. [20].

2.4. Resumen

En este capítulo se entendió como se comunicaban dos equipos a través de Internet, se conocieron algunos de los protocolos utilizados con este propósito, con especial énfasis en BGP. Además se revisaron las investigaciones y herramientas desarrolladas para medir la calidad de Internet. Con estos conocimientos es posible abordar el siguiente capítulo, donde se describe el procedimiento que se empleó para medir, desde la deficinión de la métrica, hasta los pasos necesarios para llevar la medición a cabo.

Capítulo 3

Procedimiento

En el capítulo anterior se vio como se comunicaban dos equipos en Internet, mencionando distintos protocolos y profundizando en BGP. En este capítulo se explicarán como se utilizó BGP para medir la visibilidad, desde la definición adoptada de visibilidad, hasta el diseño del sistema usado para medirla.

3.1. Introducción

La *visibilidad* de una red se entiende como el porcentaje de los routers del mundo que es capaz de ver esta red en un momento dado, es decir conoce una ruta válida desde su dirección hasta la red. Para medir esto se elige un conjunto de routers.El criterio para elegir el conjunto de routers fue elegir un conjunto tal que cubra geográficamente la mayor parte del mundo, para poder tener una visión amplia. Cabe preguntarse si sería pertinente medir con respecto a la densidad de Internet, es decir medir con respecto a más routers en, por ejemplo Japón que en África. En una primera versión no se hará, pero no se descarta como trabajo futuro.

3.2. Recolección de datos

Para medir la visibilidad de las redes chilenas en el mundo, se necesita obtener la información sobre las redes chilenas en servidores del mundo. Existen dos modos posibles de obtener

estos datos:

1. Conectarse a los "looking glasses" y consultarlos directamente.

2. Obtener la información a partir de los recolectores.

Para saber qué camino tomar, se desarrollaron prototipos de ambas alternativas, tanto consultar a los "looking glasses", como obtener información de recolectores.

3.2.1. Prototipo looking-glasses

El prototipo para conectarse a los "looking glasses" consistió en un programa en Java que se conectaba mediante telnet a cada servidor y preguntaba por cada una de las redes chilenas. El proceso de consulta tomaba del orden de horas. Aunque se podría mejorar el rendimiento, haciendo consultas de manera concurrente, se decidió realizar el prototipo para el otro método para comparar antes de seguir avanzando en esta dirección. Un resultado de ejemplo de esta consulta se presenta a continuación.

```
route-views.optus.net.au>show ip bgp 192.80.24.6
BGP routing table entry for 192.80.24.0/24, version 15991405
Paths: (3 available, best #1, table Default-IP-Routing-Table)
  Not advertised to any peer
  7473 6762 6429 23140
    202.160.242.71 from 202.160.242.71 (202.160.242.71)
      Origin IGP, localpref 100, valid, external, best
      Community: 7473:22015 7473:32915
  7474 7473 6762 6429 23140
    203.13.132.53 from 203.13.132.53 (172.26.32.13)
      Origin IGP, localpref 100, valid, external
      Community: 7473:22015 7473:32915 7474:1403
  7474 7473 6762 6429 23140
    203.13.132.35 from 203.13.132.35 (172.26.32.42)
      Origin IGP, localpref 100, valid, external
      Community: 7473:22015 7473:32915 7474:1403
```

3.2.2. Prototipo recolectores

El prototipo para obtener la información de los recolectores, consistió en un programa para descargar los archivos más recientes y un programa para procesar estos datos y encontrar las redes que fueran anunciadas por Sistemas Autónomos chilenos.

3.2.3. Discusión

El realizar estos prototipos, permitió conocer las ventajas y desventajas reales que ambos métodos tienen, cosa que no es posible a priori, y sin consumir los recursos que hubiese sido costado elegir un camino inmediatamente.

El conectarse a los "looking glasses" tiene la ventaja de poder medir en tiempo real lo que sucede, tiene la desventaja de consumir recursos de red, y tener tiempos de respuesta dependientes de sistemas externos, es decir, la velocidad de respuesta que se pueda obtener depende del tráfico que tenga cada servidor. Además, varios de los servidores "looking glasses" prohíben la conexión automática (mediante scripts o bots), para evitar un sobreuso de sus redes, y aunque otros no lo prohíben, queda la sensación de estar haciendo un daño.

Por otro lado, al obtener la información a partir de los recolectores, se obtienen datos con mayor antigüedad, pues son publicados cada cinco minutos las actualizaciones y cada 8 horas las tablas completas. Además se deben filtrar y preprocesar los datos para obtener aquellos relevantes a este estudio en particular, pues el formato de los datos no es texto simple y vienen datos de todas las redes, no solamente las redes chilenas.

Se decidió usar la alternativa recolectores pues se pretende generar estadísticas históricas, por lo que no se considera necesario tener datos de último minuto, pero sí que el sistema pueda responder rápidamente a las consultas que se hagan posteriormente sobre los datos ya procesados. Además se tiene la opción de realizar el estudio para meses pasados, y no sólo hacia el futuro.

Se obtendrán las tablas de rutas una vez al día, y con esta información se irá construyendo

una base de datos con la información de la visibilidad, analizando diariamente.

Como punto de inicio se pidió el registro completo WHOIS a LACNIC (Bulk WHOIS), que contiene la información sobre las IPs y Autonomous System Number asignadas en la región. De esta forma se puede saber cuáles son las redes y los Sistemas Autónomos chilenos y a quién pertenecen. LACNIC publica un resumen que contiene las redes y el país [16], con esto se podría ir actualizando parcialmente la base de datos, para descubrir la empresa a la que pertenece, habría que usar el comando WHOIS para cada nueva red.

Se decidió utilizar las tablas BGP, obtenidas desde RIPE, pues cuenta con 13 recolectores activos repartidos ampliamente en el mundo (ver Cuadro: 3.1), que se comunican con alrededor de 200 Sistemas Autónomos. Cada recolector tiene una sesión BGP con algunos Sistemas Autónomos, y de esta forma obtiene información sobre las rutas a las que estos pueden llegar. El usar recolectores de RIPE, asegura que todos los datos estén en el mismo formato, lo que facilita su procesamiento.

Recolector	**Ubicación**
rr00.ripe.net	Ámsterdam, Países Bajos
rrc01.ripe.net	Londres, Inglaterra
rrc03.ripe.net	Ámsterdam, Países Bajos
rrc04.ripe.net	Génova, Italia
rrc05.ripe.net	Viena, Austria
rrc06.ripe.net	Otemachi, Japón
rrc07.ripe.net	Estocolmo, Suecia
rrc10.ripe.net	Milán, Italia
rrc11.ripe.net	New York, Estados Unidos
rrc12.ripe.net	Frankfurt, Alemania
rrc13.ripe.net	Moscú, Rusia
rrc14.ripe.net	Palo Alto, Estados Unidos
rrc15.ripe.net	Sao Paulo, Brasil
rrc16.ripe.net	Miami, Estados Unidos

Cuadro 3.1: Ubicación de los recolectores utilizados

3.3. Problemas de medición

En primera instancia, se pensó que se podría medir la visibilidad con respecto a los 200 Sistemas Autónomos conectados a los recolectores. Sin embargo, luego de intentarlo y

obtener resultados extraños (visibilidades que no superaban el 1 %) se descubrió que había algún problema con la mediciíon. Se realizó un análisis en conjunto con expertos, estudiando casos claves y se pudo detectar el problema: hay rutas que no son anunciadas al recolector, por lo que la visibilidad sólo puede ser medida para los recolectores y no para todos los Sistemas Autónomos vecinos a ellos.

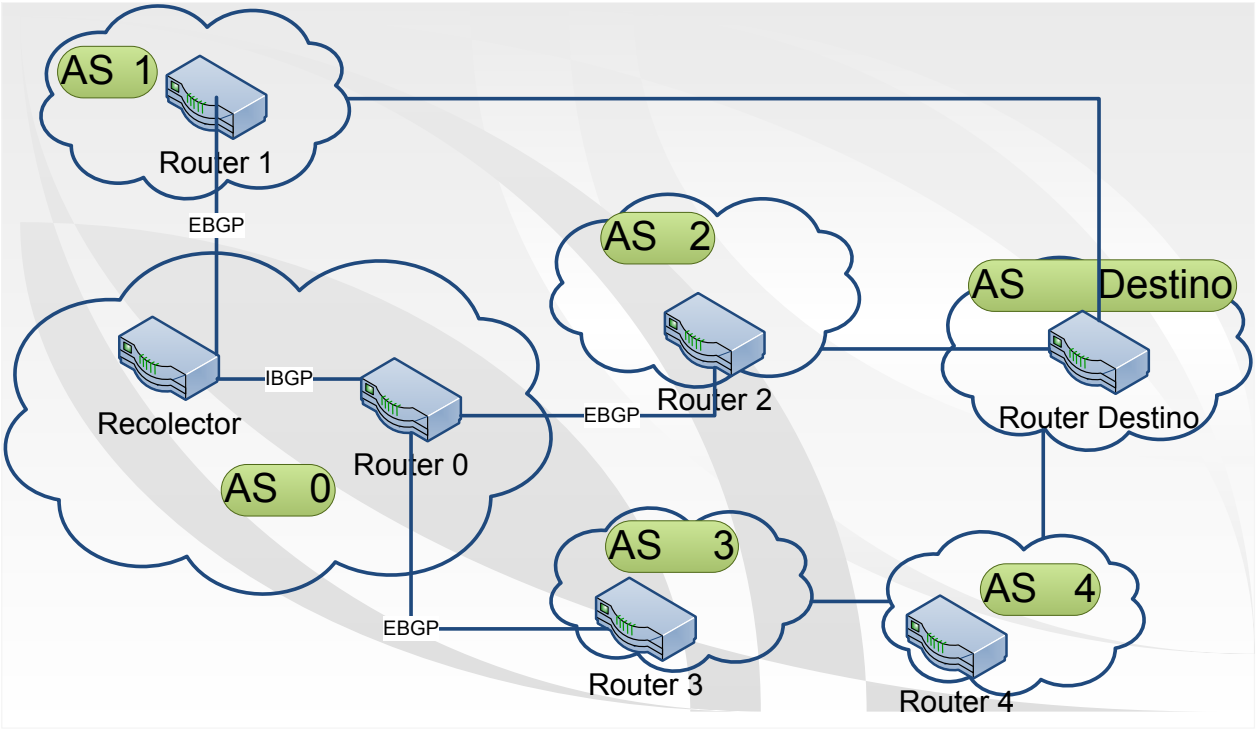

Figura 3.1: Ejemplo de configuración del Sistema Autónomo de un recolector

El problema expuesto anteriormente se ejemplifica en la figura 3.1, donde se describe una posible topología de un recolector. El *recolector* pertenece al mismo Sistema Autónomo que el *router 0*, además el *recolector* mantiene una sesión BGP con el *router 1*, del *Sistema Autónomo 1* y con el *router 0*, de su mismo Sistema Autónomo.

Por otro lado el *router 0* tiene una sesión BGP con los *routers 2 y 3* , de los *Sistemas Autónomos 2 y 3* respectivamente.

Así para llegar a la *red destino*, hay 3 caminos posibles, usando el *Sistema Autónomo 1*, usando el *Sistema Autónomo 2* o usando el *Sistema Autónomo 3*. Al recolector se le comunica externamente (EGP, externo a su Sistema Autónomo) el camino {*AS1,AS Destino*}.

Al *router 0* se le comunican dos caminos: {*AS2,AS Destino*} y {*AS3, AS4, AS Destino*}. El *router 0*, elige uno de estos dos caminos (el mejor) para comunicárselo internamente al Recolector (IGP, interno a su Sistema Autónomo), en este caso el camino {*AS2, AS Destino*}. Por lo tanto el recolector no sabe que el *Sistema Autónomo 3* también puede llegar a la *red destino*.

En conclusión la visibilidad no puede ser medida para otros Sistemas Autónomos desde el recolector, sino que sólo se puede medir visibilidad para el recolector mismo, pues hay rutas que existen y que quedan ocultas debido a que no son anunciadas por no ser consideradas la *mejor* ruta. En este estudio se se medirá la visibilidad con respecto a los 13 recolectores RIPE activos.

3.4. Procesamiento de datos

De las tablas BGP, que los recolectores mantienen disponibles públicamente, se obtienen los dos datos relevantes para este estudio:

1. La red destino
2. El camino de Sistema Autónomo (AS path), que es la lista de los Autonomous Systems por los que debe pasar para llegar hasta la red.

Lo que en este trabajo se estudia es si se puede llegar a las redes chilenas, por lo que, en principio, del AS path, interesa simplemente el último Sistema Autónomo, es decir el destino, que debería ser un Sistema Autónomo chileno. Pero además se pretende saber si esa ruta es correcta.

Para poder determinar esto último, se necesitaría conocer la topología completa de la red, es decir qué par de Sistemas Autónomos son vecinos, para poder chequear que el AS path sea correcto, lamentablemente esto escapa del alcance de esta memoria, por lo que se decidió verificar desde el punto en que se ingresa a Chile, pues se busca detectar si hay algún error de ruteo específicamente en Chile.

El método elegido de lograr este objetivo es entrenar el sistema y complementar esto con los datos obtenidos desde Cyclops [20], para conocer la topología chilena, es decir cuales Sistemas Autónomos están conectados. Se inicializó el sistema con los datos que mantiene Cyclops, los vecinos que tuvieran al menos una semana de antiguedad, luego durante una semana se aceptaron los AS Path y se guardaron como caminos válidos, luego de este periódo, los nuevos caminos deben ser agregados manualmente. De esta forma si se detecta que hay una ruta que pasa por dos Sistemas Autónomos que no están conectados, esa ruta es posiblemente errónea y será reportada como tal, para que al revisar los datos, se incluya como un camino válido, o se comunique al Sistema Autónomo involucrado.

3.4.1. Procedimiento de medición

Luego de tener todos los AS Paths desde todos los recolectores hasta todas las redes, hay que filtrar para obtener sólo las redes chilenas. Este proceso no es tan simple como hacer una búsqueda en la lista de redes chilenas, pues también es correcto anunciar subredes, es decir un subconjunto de la red que se posee.

Por ejemplo si se tiene la red de la figura 3.2: *200.24.0.0/16*, se puede anunciar esta red completa, una o ambas subredes: *200.24.0.0/17*, *200.24.128.0/17*, o alguna(s) de las múltiples subredes de éstas, incluso se puede anunciar una red y además sus subredes, por ejemplo anunciar las dos subredes a un Sistema Autónomo y anunciar la red a otros Sistemas Autónomos, como respaldo ante alguna eventualidad.

Para entender cómo funciona esto, hay que recordar que cada red es un conjunto de IPs, si se desea anunciar un subconjunto de esta red, el conjunto se divide en 2 partes iguales, obteniendo dos redes con un largo de máscara igual al largo de la máscara de la red original más uno. Este proceso puede repetirse hasta llegar al tamaño de la red que uno desee anunciar, en cada iteración, el tamaño de la red se divide a la mitad.

En el caso de Chile, según el Bulk Whois [16], existen 6838 redes chilenas, pero muchas estas redes son en realidad subconjuntos de otras redes de esta misma lista, por lo que se estaría contando más de una vez cada IP. Lo que se busca es un conjunto de redes tal que

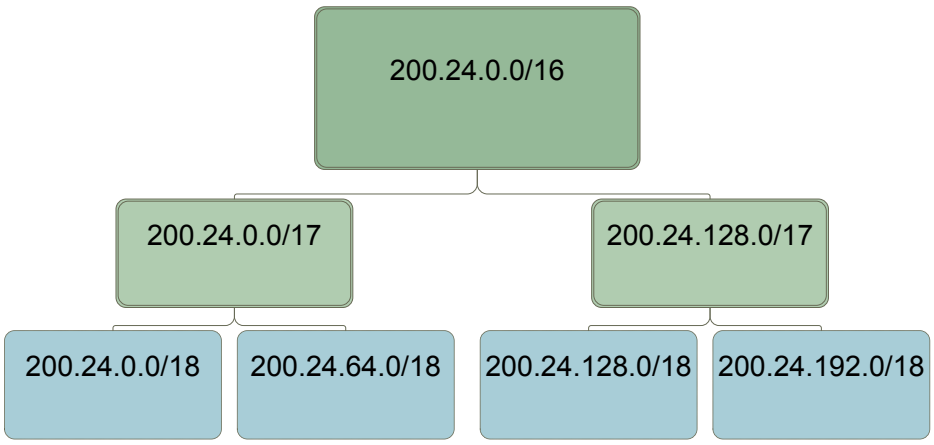

Figura 3.2: Tres niveles del árbol binario de la red 200.24.0.0/16

no haya intersección entre ellas, es decir que no haya una IP que pertenezca a dos redes. Solo 696 de estas redes no tienen como superred otra red chilena, es decir hay 696 conjuntos disjuntos de IPs en Chile. Son estos conjuntos los que se estudian en la presente investigación, agrupados por empresa a la que pertenecen.

Una red, o una subred, se considerará *anunciada*, si es visible desde algún recolector. Esta definición se adoptó pues la única forma de saber si una red está siendo anunciada, es verla desde algún lugar (verla en alguna tabla de rutas). Notar que el que una red sea anunciada significa que esa red está activa, está siendo utilizada con algún fin. En cambio si la red no es anunciada, el resto del mundo no puede contactarse con ella, lo que significa que esa red no está siendo utilizada, o no existe ninguna forma de llegar a ella.

Para saber cuánto de la red es anunciado, se debe tener en cuenta si la red fue anunciada, o si fue anunciada alguna de sus subredes, teniendo en este último caso en consideración el tamaño de la subred anunciada.

Para obtener la visibilidad, se toman las redes anunciadas (si una red no fue anunciada es imposible que sea visible), y se mide cuánto de cada red es visible desde cada recolector,

es decir si el recolector tiene en su tabla de rutas toda la red, o una o más de sus subredes. Si no tiene la red ni ninguna de sus subredes, este recolector no sabe cómo llegar a la red, y por lo tanto esa red no es visible para él.

Lo anterior corresponde a la visibilidad de la red por recolector, para calcular la visibilidad total de la red se promedia la visibilidad por recolector.

$$v_{red_i} = \frac{\sum_{j \in Recolectores} v_{ij}}{\#Recolectores} \tag{3.1}$$

v_{ij} : Visibilidad de la red i en el recolector j

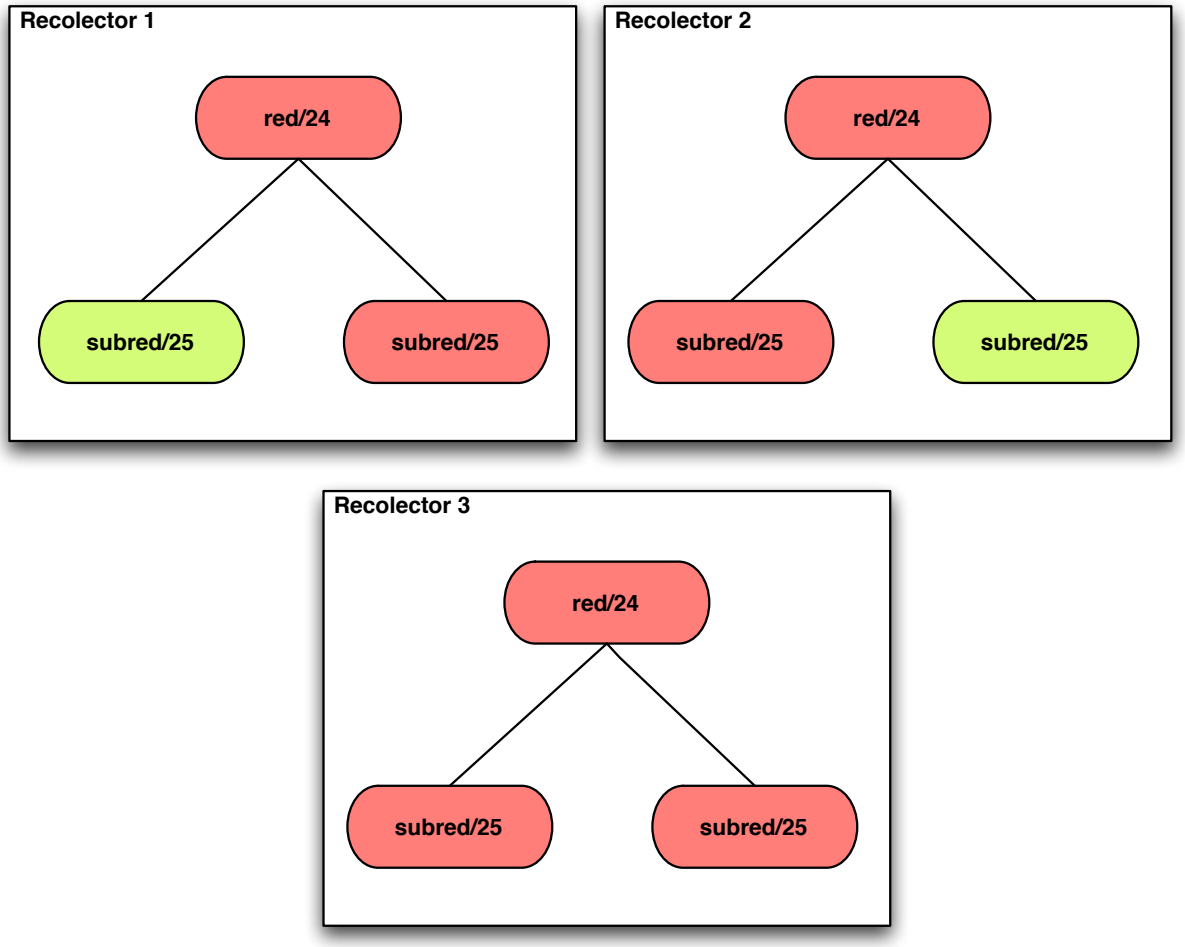

Figura 3.3: Ejemplo de conceptos de visibilidad (33,33 %) y anunciado (100 %)

Para entender los conceptos de anunciado y visibilidad, tomemos como ejemplo la configuración de la figura 3.3, con tres recolectores, donde el color verde indica que esa red

está presente en el recolector y el color rojo representa que no está en su tabla. En el recolector 1 está presente una de las dos subredes, en el recolector 2 está la otra subred, y en el recolector no hay ningún bloque presente. Dado que las dos subredes están presentes en algún recolector, se tiene que el porcentaje anunciado es del 100 %.

Del total anunciado (la red completa), el recolector 1 tiene sólo una subred, que representa el 50 % del total, lo mismo ocurre con el recolector 2, ambos tienen entonces un 50 % de visibilidad, mientras que el recolector 3 tiene una visibilidad de 0 %. La visibilidad total de la red se calcula como el promedio entre las visibilidades por recolector, en este caso sería: $\frac{50\,\%+50\,\%+0\,\%}{3} = 33,33\,\%$.

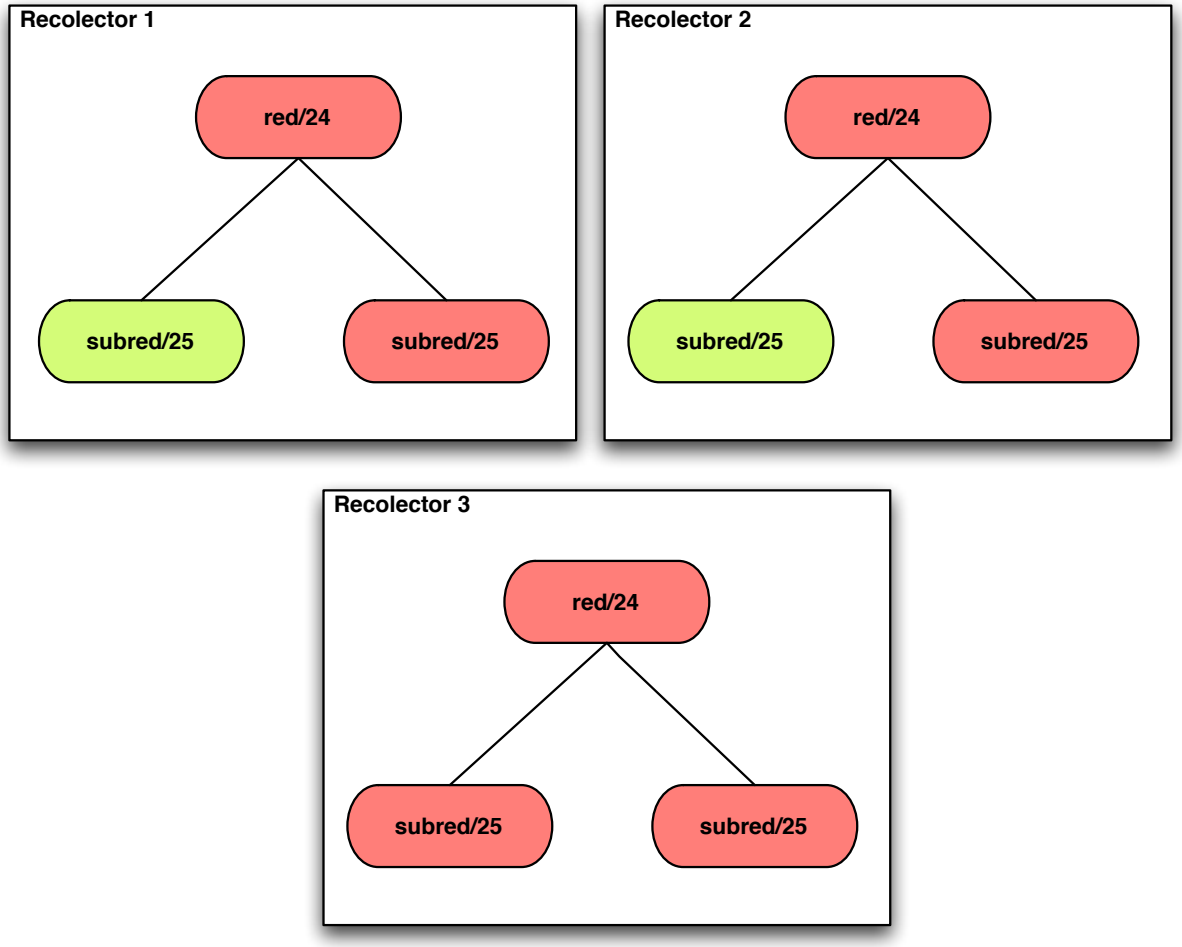

Figura 3.4: Ejemplo de conceptos de visibilidad (66 %) y anunciado (50 %)

En cambio en la configuración de la figura ejemplo 3.4 se tiene que en las tablas del recolector 1 y 2 aparece la misma subred, mientras que en el recolector 3 no aparece ninguna

de las subredes. En este escenario, tenemos que el porcentaje de red anunciado es del 50 %, y el recolector 1 y el recolector 2 tienen 100 % de visibilidad, pues ven el 100 % de lo anunciado, el recolector 3 tiene 0 % de visibilidad. Entonces la visibilidad total de la red es $\frac{100\,\%+100\,\%+0\,\%}{3} = 66.67\,\%$.

De esta forma se obtienen dos datos: el porcentaje de la red anunciada, y el porcentaje de la red anunciada que es visible desde cada recolector, estos datos son guardados en una base de datos para su posterior consulta y visualización.

3.5. Visualización de datos

Finalmente los datos son desplegados en una página web, donde se grafican los resultados para su mejor visualización. Entre los datos que se pueden revisar están las relaciones entre los Sistemas Autónomos chilenos, es decir quién provee a quién, además se pueden ver todas las redes chilenas, agrupadas por la empresa a la que pertenecen.

Los datos de la visibilidad pueden ser vistos por fecha a nivel país y a nivel de recolector y también a nivel de empresa dueña de un conjunto de redes. Al visualizarlo a nivel de empresa, se puede revisar la información histórica, ya sea por día (los últimos 30 días) o el promedio mensual (los últimos 24 meses). Además se puede revisar el detalle, es decir qué porcentaje de cada red está presente en cada recolector.

3.6. Conclusiones

Como conclusiones de este capítulo, se tiene que el método elegido para obtener los datos es descargarlos desde los recolectores RIPE, pues se generan con una frecuencia que se considera suficiente para el desarrollo de la investigación, y permite realizar análisis para fechas en el pasado.

También se averiguó que con el método adoptado, la visibilidad puede ser medida sólo con respecto a los recolectores, y no con respecto a los Sistemas Autónomos, como se pensó en

un principio, pues existen rutas que permanecen ocultas a los recolectores.

Adicionalmente se definieron los conceptos de *anunciado* y *visibilidad* de una red, con respecto al tamaño de las subredes presentes en las tablas de ruta de los recolectores.

3.7. Resumen

En este capítulo se vio la definición de lo que se medirá: porcentaje de las redes anunciado y visible, así como también como se pretenden medir estos indicadores sobre las redes chilenas. Se vio también una primera división del sistema que se utilizará para medir. En el próximo capítulo se revisan detalles de la implementación que aclaran en profundidad el desarrollo del sistema, cómo se mide y cómo se muestran estos datos.

Capítulo 4

Implementación

En el capítulo anterior, se vieron las definiciones de lo que se medirá y cual es el procedimiento utilizado para hacerlo. En este capítulo se verá la implementación de este procedimiento, desde la recolección de los datos, hasta la visualización de los datos ya procesados. Se justifican las desiciones tomadas, como el uso de un lenguaje de programación específico para cada parte, así como también las arquitecturas usadas en las distintas partes del sistema.

4.1. Arquitectura de alto nivel del sistema

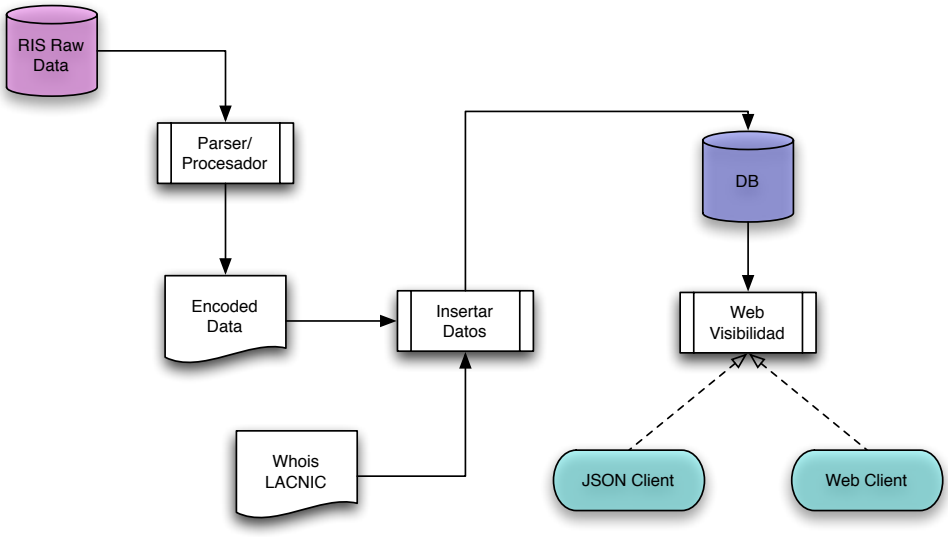

Figura 4.1: Arquitectura del sistema

El sistema se dividió en tres partes: recolección de datos, procesamiento de los datos y visualización de los datos (fig: 4.1).

4.1.1. Recolección de datos

La recolección de los datos fue hecha usando el programa wget. Este programa recibe una URL y descarga este archivo desde internet. Se creó un programa que genera los nombres de los archivos a descargar, y luego invoca a wget con los nombres generados anteriormente.

Las tablas BGP, sólo se pueden descargar en un formato conocido como MRT. [3]. Dentro de lo investigado, se encontró sólo una biblioteca para entender este formato. Esta biblioteca existe en dos versiones, para el lenguaje C, llamada libbgpdump [2] y para el lenguaje Phyton, lamentablemente ésta última versión no se logró utilizar, por problemas de compatibilidad; por este motivo, esta parte del sistema fue desarrollada en el lenguaje C.

Los archivos descargados son entonces preprocesados, para obtener los datos relevantes, por un programa hecho en C, para comunicarse directamente con la biblioteca libbgpdump. Este programa, se usa para generar un archivo que contiene en cada línea una red y su AS Path.

4.1.2. Procesamiento de datos

El procesamiento de este archivo de texto fue hecho usando Java, se crearon los objetos:

- Red
- Superred
- Empresa
- Sistema Autónomo
- Medición

- Medición por recolector
- Resumen diario

Estos objetos, usando Java Persistence API (JPA) son traducidos a un modelo entidad relación, lo que permite abstraerse de la interacción con la base de datos y sólo trabajar en el ámbito de los objetos.

JPA permite trabajar con múltiples bases de datos y frameworks, en este trabajo en particular se utiliza una base de datos MySQL y el framework Hibernate, que se encarga de hacer el mapeo (traducción) entre los objetos y las entidades.

Se decidió usar una base de datos, pues es una forma concreta de almacenar la información, que permite ser accedida tanto desde una página web, como desde otros programas, separando el problema del almacenamiento de datos del problema de la generación, procesamiento y visualización de éstos.

Para poder separar eficientemente el proceso de generación del proceso de almacenamiento de los datos se utilizó JPA, por este motivo, y por la familiaridad con el lenguaje, se eligió utilizar Java para hacer el desarrollo de esta parte del sistema.

Para verificar que una red haya sido correctamente anunciada, es decir que el AS Path sea válido, hay que saber qué Sistema Autónomo puede anunciar cada red y cuáles Sistema Autónomo son vecinos. Para saber esto, se inicializó el sistema, aceptando como válidas todas los caminos durante una semana, adicionalmente se complementaron estos datos con datos obtenidos desde la herramienta Cyclops [20]. Este proceso es continuo, al correr diariamente el sistema, genera alertas avisando las rutas que le parecen erróneas, se debe manualmente aceptar la ruta como válida agregándola a la base de datos, o investigar más profundamente en caso de que sea una ruta errónea (avisando a los Sistemas Autónomos involucrados).

4.1.3. Visualización de datos

La visualización de los datos fue realizada usando CakePHP [6], pues uno de los objetivos del sistema es que la información sea pública, y para esto, un buen método es publicarla en Internet.

Se diseñó una página web que permite revisar los datos generados por el sistema, de esta manera, se permite que cualquiera pueda revisar ya sea su propia visibilidad o la de el resto de las redes chilenas y pueda usar estos datos para otro tipo de estudios, o para mejorar o reparar sus configuraciones. CakePHP tiene la ventaja de ser suficientemente simple para crear páginas que interactúan fuertemente con bases de datos, y tiene la flexibilidad necesaria para poder visualizar los datos de la forma que se estimó adecuada.

Para graficar los datos, se usó la API de Google Chart [13], la que recibe una url y devuelve el gráfico como imagen. Esta desición se tomó pues es una forma simple, ordenada y bastante potente de generar gráficos a partir de datos.

4.2. Análisis detallado del sistema

En la figura 4.1, se vieron las distintas partes del sistema, cada una de estas partes se explicará a continuación.

4.2.1. Recolección de datos

En la figura 4.2 se muestra el detalle del proceso de recolección de datos.

El primer programa (downloader.c) es el que genera los nombres de los archivos a bajar. Para esto pide al sistema la fecha y hora actual, calcula cuál fue el último archivo generado, generando la url del archivo y el nombre con el que se bajará (para reemplazar al del día anterior). Luego llama a wget, usando un fork-exec descargando así los datos necesarios.

El programa para preprocesar (preprocesar.c) abre cada uno de estos archivos y procesa

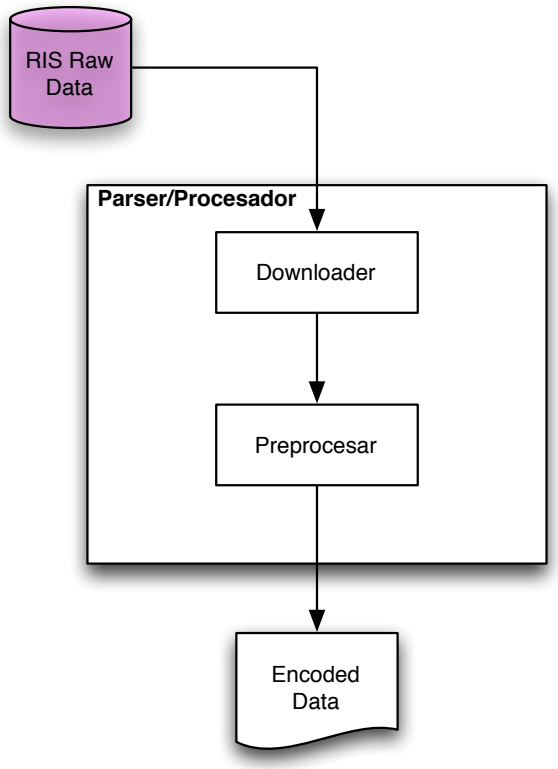

Figura 4.2: Arquitectura Recolección

cada entrada del archivo, que es una entrada en la tabla BGP del recolector. El procesamiento consiste en obtener la red de destino y el camino de Sistemas Autónomos e imprimirlo. Esto se guarda en un archivo, que luego será procesado por el programa en Java.

4.2.2. Procesamiento de datos

En la figura 4.3 se detallan las interacciones entre las componentes del subsistema de procesamiento. El programa que procesa (TestAllPaths.java), carga en memoria todas las superredes chilenas y todos los recolectores, luego lee cada línea del archivo resultante del proceso anterior, es decir los datos ya preprocesados, revisa si la red destino es chilena, es decir si es subred de alguna de las superredes chilenas.

El diagrama de clases se muestra en la figura: 4.4, allí se ven, no sólo las clases de almacenamiento de datos, sino que también las que se utilizan para el procesamiento de éstos.

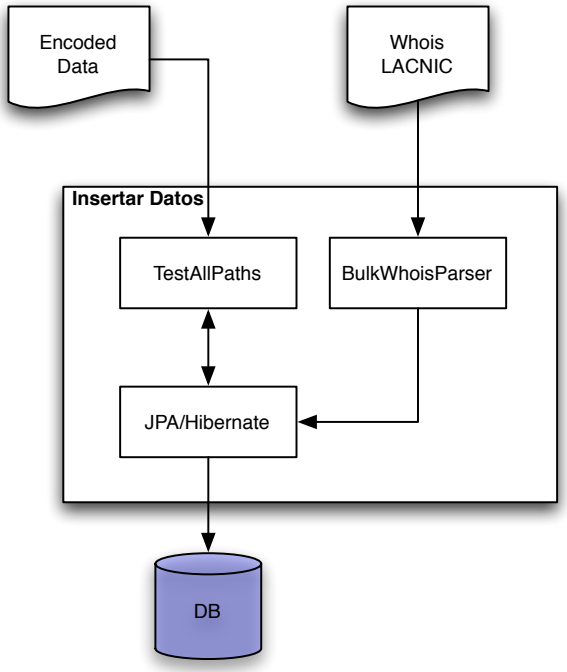

Figura 4.3: Arquitectura Procesamiento

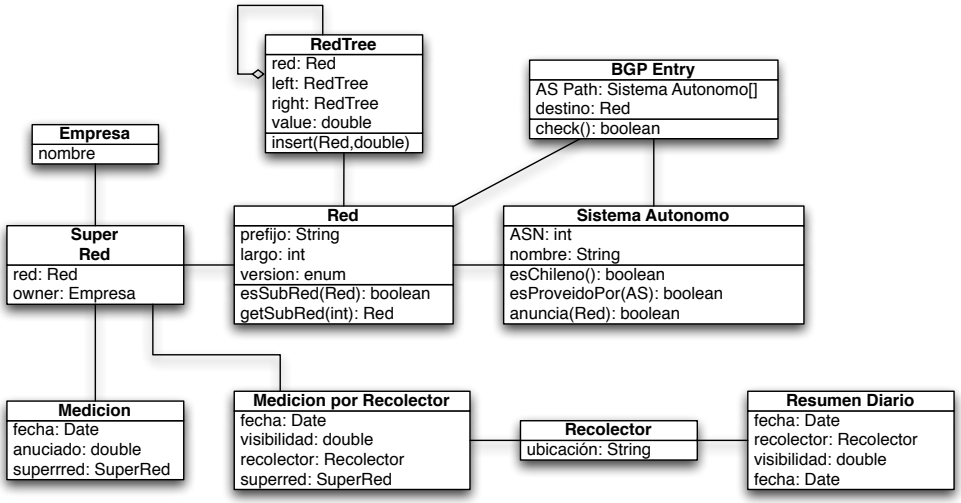

Figura 4.4: Diagrama de clases del subsistema de procesamiento de datos

Con el objeto de determinar eficientemente tanto si una red es subred de alguna red que interesa a este estudio (las redes chilenas) como el aporte relativo al total que significaba, se creó una estructura tipo árbol, similar al de la figura 3.2, pero que además incluye un valor entre 0 y 1 que representa ya sea lo *anunciado* o la *visibilidad* dependiendo del caso de uso.

La estructura del árbol es la siguiente:

Campo	Descripción
red	Superred del árbol.
value	Número entre 0 y 1, que representa la visibilidad o lo anunciado según el caso.
left	Árbol con las subredes con IPs más bajas.
right	Árbol con las subredes con IPs más altas.

Se creó una lista ordenada de árboles de redes (conocido como bosque, por ser un conjunto de árboles) donde las raíces de los árboles de la lista son las superredes chilenas.

Para cada entrada de las tablas de rutas, usando el bosque de superredes, se realiza una búsqueda binaria de la red sobre las raíces, pero en vez de usar el compararador de igualdad, se utiliza la comparación de subconjunto, es decir si el elemento es subconjunto de la raíz (si la red es subred de la raíz). En caso de que no sea subconjunto de ninguna superred chilena, la red no es chilena y termina su procesamiento (se sigue con la siguiente). En cambio, de sí ser subred de alguna red, se inserta el elemento bajo la superred correspondiente, con valor 1 en el campo *value* y se recalcula este valor hacia la raíz.

El cálculo es el siguiente: en cada nivel se recalcula como el máximo entre el valor actual y la semisuma de las visibilidades de los hijos, es decir el promedio. Se tiene un valor por red, que es lo anunciado, y un valor por red por recolector, que es la visibilidad. Se tiende a pensar que lo anunciado es el máximo de las visibilidades, y muchas veces será así, pero en el caso general, se puede tener cierta subred visible desde un recolector y otra subred visible desde otro recolector, de forma que lo anunciado sea mayor al máximo de las visibilidades.

El pseudo código del programa es el siguiente:

```
List(n): redes_chilenas
List(m): recolectores
Matrix(n , m) : visibilidad
Bosque(n): bosque_visibilidad , bosque_anunciado

foreach( red in redes_chilenas ):
  Agregar red a bosque_visibilidad como un Arbol de Redes;
  Agregar red a bosque_anunciado como un Arbol de Redes;
```

```
endforeach

foreach( recolector in recolectores ):
  foreach( BGPEntry for recolector ):
    i = pertenece(redes_chilenas, BGPEntry.red, 0, n);
    if i >= 0 then:
      check( BGPEntry );
      bosque_visibilidad[i].insert(BGPEntry.red,1);
      bosque_anunciado[i].insert(BGPEntry.red,1);
    endif
  endforeach
  for i in 0..n
    visibilidad(i,recolector) = bosque_visibilidad[i];
    bosque_visibilidad[i].reset();
  endfor
endforeach
```

Las visibilidades son con respecto a cada recolector, por eso se resetea es decir se vuelve a poner en 0 el valor del árbol al cambiar de recolector, por otro lado, lo anunciado es global, por lo que se mantienen los datos, y se va actualizando con cada recolector.

La función *pertenece* es una búsqueda binaria, con la única diferencia del comparador, en vez de utilizar la igualdad, se usa la relación: ser subred.

Para saber si una red es subred de otra, hay que primero revisar el largo de las máscaras, luego se aplica la máscara a cada prefijo, y se comparan estos resultados.

```
esSubRed(subRed, superRed){
  if( subRed.mask.largo>superRed.mask.largo)
    return false;
  return subRed.prefijo & subRed.mask == superRed.prefijo & subRed.mask;
}
```

La base de datos, tiene el modelo de la figura: 4.5. Este modelo fue definido por la JPA, al

crear los objetos. La tabla *autonomous_systems_autonomous_systems* se usa para almacenar las relaciones entre los Sistemas Autónomos, es decir cuáles Sistemas Autónomos son vecinos y quién provee a quién. Así mismo la tabla *autonomous_systems_chilean_networks* almacena qué Sistemas Autónomos pueden anunciar que redes.

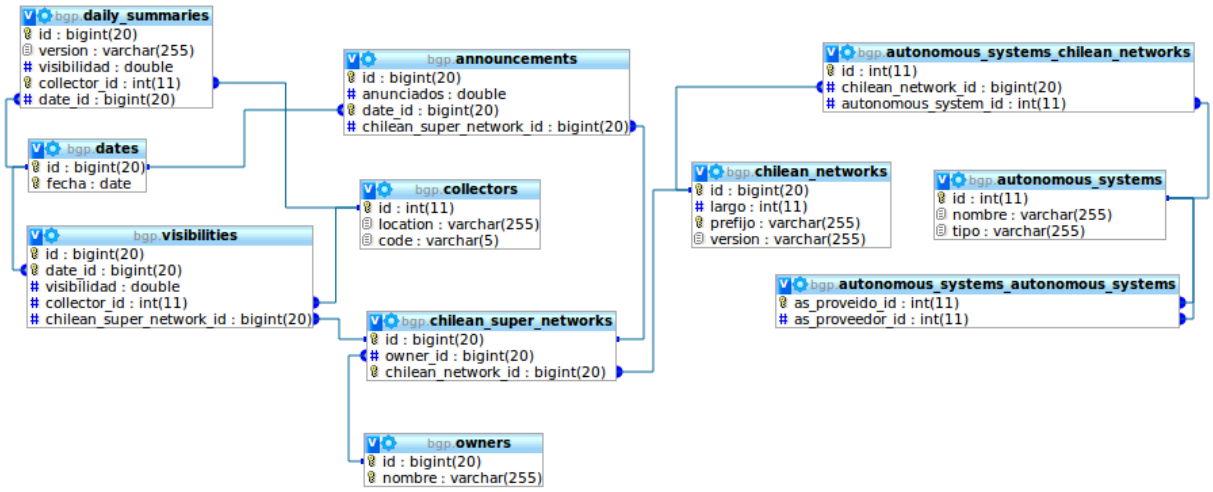

Figura 4.5: Diagrama de la base de datos.

Se almacena además un resumen diario a nivel país por recolector, esto pues, si bien es redundante, acelera las consultas. A futuro se pueden almacenar otros datos agregados, para liberar de carga al servidor web.

Como el subsistema de procesamiento de datos está hecho con JPA, los objetos en Java son las entidades del modelo relacional. Además hay otros objetos, como los ya mencionados árbol de redes, y *BGPEntry*, que sirve para almacenar y verificar una entrada de los datos preprocesados, es decir una red de destino, y un camino de Sistemas Autónomos. *BGPEntry*, chequea que los Sistemas Autónomos chilenos del camino, estén conectados, en caso contrario se genera una alerta. Es una alerta y no un error, ya que, que el sistema no los reconozca como vecinos no implica que no sean efectivamente vecinos, pues como ya se explicó, puede ser un vecino nuevo o uno que se mantuvo oculto.

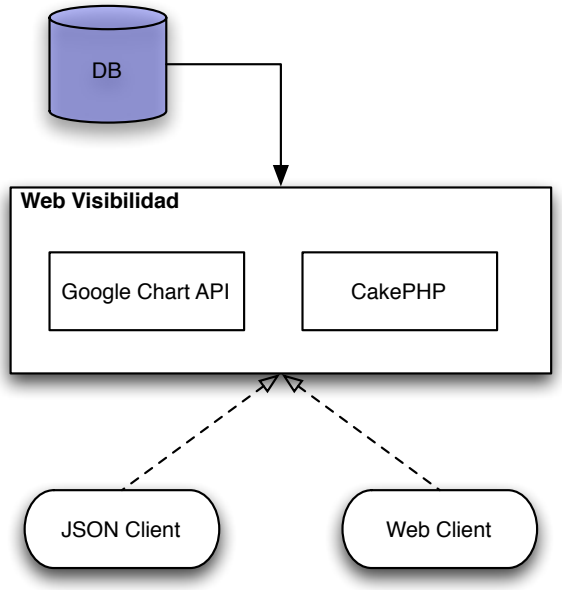

Figura 4.6: Arquitectura Visualización

4.2.3. Visualización de datos

En la figura 4.6 se aprecian las componentes del susbistema de visualización web, que toma los datos de la base de datos y los despliega en un sitio web. En el subsistema de visualización, se siguió el modelo vista controlador, implementado en CakePHP según la figura 4.7. Donde cada tabla de la base de datos (mysql), se traduce a un modelo, cada modelo tiene asociado un controlador que es donde está la lógica de ese modelo y cada función del controlador tiene una vista que es el despliegue de los datos. Dentro de un controlador hay múltiples funciones, las funciones comunes a todos los modelos son dos: *index*, y *view*. *Index* despliega todas las filas de la tabla que representa el modelo y *view* muestra una fila de la tabla, y las entidades relacionadas, por ejemplo, de una empresa, muestra las redes que le pertenecen.

Las otras funciones desarrolladas son *summarize*, del modelo Empresa (*Owner*) y del modelo Fecha (*Date*) que hacen los promedios y grafican los datos. *Summarize* en el controlador de Empresa tiene dos modos: *por día*, que muestra los últimos treinta días y *por mes*, que muestra el promedio mensual de los últimos veinticuatro meses.

Los valores de redes anunciadas y visibles, se almacenan como un valor entre 0 y 1. Al momento de desplegar los datos, en el servidor web, se calculan los promedios ponderados

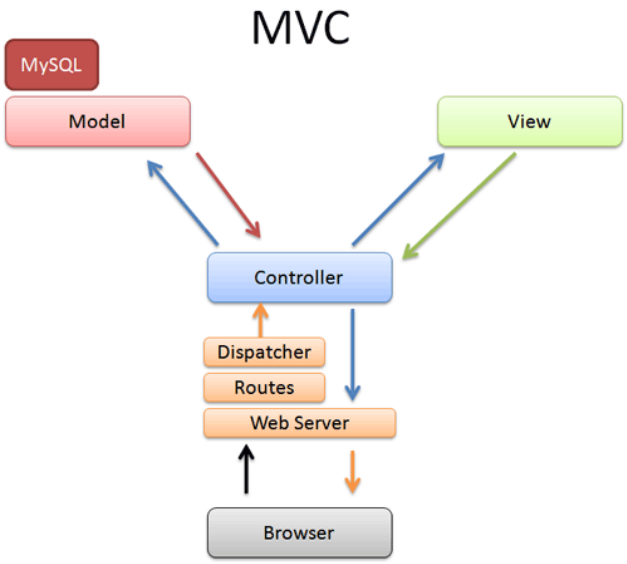

Figura 4.7: Modelo Vista Controlador en CakePHP.

para cada empresa. La ponderación se calcula con respecto al tamaño anunciado de la red (ver (4.1)) pues una red más grande, contiene un mayor número de IPs, es decir podría tener más equipos, además se multiplica por lo anunciado, para obtener un número entre 0 y *anunciado*.

$$Visibilidad_{Empresa} = \frac{\sum_{i \in RedesEmpresa} t_i \times v_i \times a_i}{\sum_{i \in RedesEmpresa} a_i \times t_i} \tag{4.1}$$

t_i : Tamaño de la red i

v_i : Visibilidad de la red i

a_i : Porcentaje de la red i anunciada

Así mismo, el promedio general de visibilidad de las redes chilenas, se calcula (4.2).

$$Visibilidad_{Chile} = \frac{\sum_{i \in RedesChilenas} t_i \times v_i \times a_i}{\sum_{i \in RedesChilenas} t_i \times a_i} \tag{4.2}$$

Por otro lado, para calcular el promedio de una fecha en particular, es decir el promedio diario, se usa el resumen diario por recolector, actualmente se usa el promedio simple de

todos los recolectores, pero como se mencionó anteriormente, en futuras versiones, podría ponderarse de acuerdo a la densidad de Internet, o algún otro indicador que se considere relevante.

4.3. Resumen

En este capítulo, se revisó la implementación del sistema, la división de éste en recoleccion, procesamiento y visualización de los datos. Se describió el algoritmo utilizado y los objetos creados para el procesamiento y los modelos y controladores utilizados para la visualización de los datos. En el siguiente capítulo se verán los resultados obtenidos al realizar mediciones con la herramienta desarrollada.

Capítulo 5

Resultados

En el capítulo anterior se mostró la forma en que fue implementada la herramienta para medir la visibilidad de las redes chilenas, en este capítulo se muestran y analizan los resultados obtenidos al usar esta herramienta.

5.1. Introducción

El primer resultado de este trabajo, es la herramienta en sí, que genera reportes diariamente, midiendo la visibilidad y lo anunciado a nivel de superred, empresa y país.

Una vez completado el sistema, se comenzó inmediatamente a realizar mediciones. El objetivo fue realizar la mayor cantidad de mediciones posibles, por lo que se realizaron mediciones diariamente cuando fue factible. Las mediciones se continúan realizando actualmente. Además si se quiere revisar alguna fecha específica, también se puede configurar el sistema para realizar la medición para ese día en particular.

5.2. Mediciones

Las primeras mediciones fueron hechas el día 18 del mes de noviembre de 2009. Los resultados se detallan a continuación.

Se detectó que en IPv4, se anunciaban 315 de 683 redes. En la figura 5.1 se aprecia del total de redes de cada empresa el porcentaje anunciado.

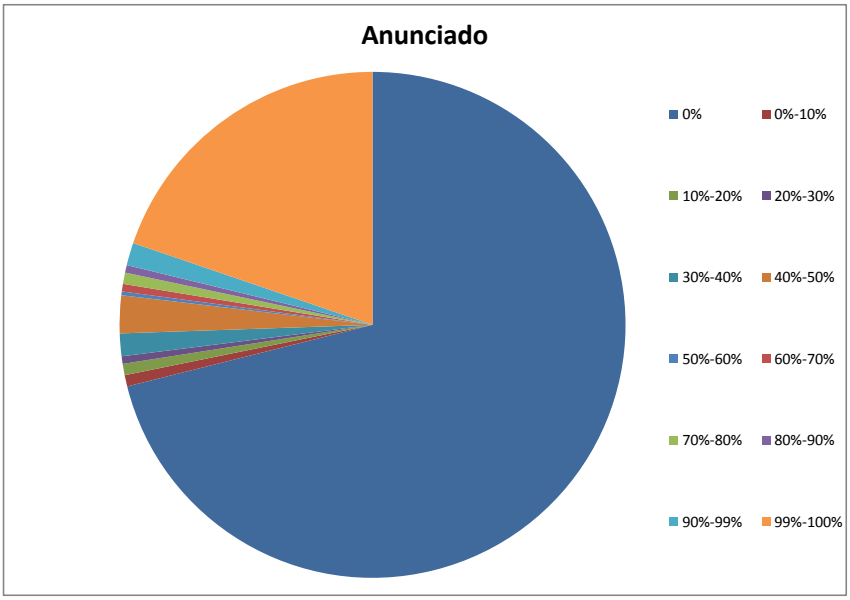

Figura 5.1: Porcentaje de las Redes Chilenas Anunciadas el 18-11-2009

Es decir más de un 70 % de las empresas no anuncia sus redes, mientras que alrededor del 20 % anuncia el 100 % de sus redes.

Con respecto a la visibilidad (en la figura 5.2), casi todas las redes anunciadas fueron visibles desde los 13 recolectores activos, a excepción de una (perteneciente a REUNA), que tuvo un porcentaje que no fue visible en 6 de los 13 recolectores. Para el primer día estudiado, la visibilidad a nivel país, resultó ser del 99,99 %.

Estos resultados muestran que las redes chilenas son poco anunciadas, lo que indica una de dos cosas: o no son usadas, o son mal anunciadas de modo que nadie puede verlas. Por otro lado, las redes anunciadas son altamente visibles, lo que indicaría, que si la red logra llegar a cierto punto, es bien distribuida por el resto de los Sistemas Autónomos.

En cambio a IPv6, hay solamente 13 redes asignadas a empresas chilenas. De éstas únicamente 6 son anunciadas. La visibilidad es bastante menor, alcanzando un 81,54 %, esto se

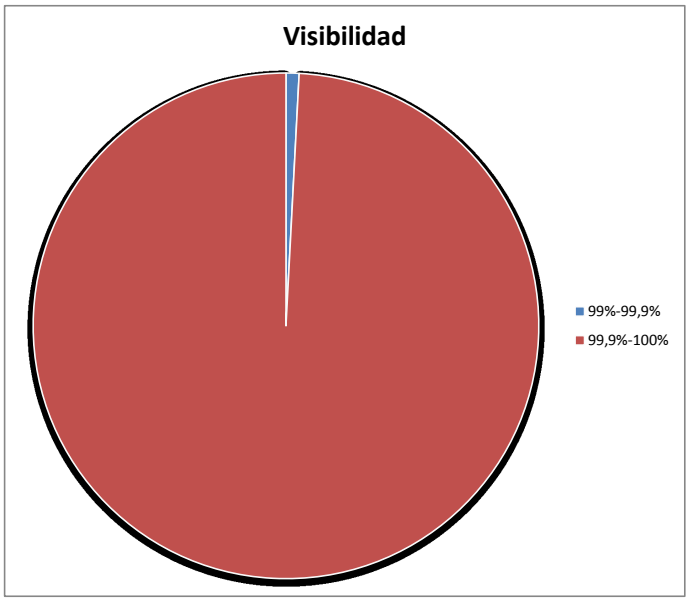

Figura 5.2: Visibilidad de las Redes Chilenas Anunciadas el 18-11-2009

explica pues hay 2 recolectores (el recolector ubicado en Otemachi, Japón y el ubicado en Moscú, Rusia) que no ven redes IPv6, ya sea por que ellos no tienen las capacidades, o sus vecinos no tienen implementado aún el protocolo, además hay otros dos recolectores que ven sólo algunas de las redes IPv6, específicamente el recolector ubicado en Sao Paulo, Brasil, y el ubicado en Miami, Estados Unidos, no ven la red IPv6 de REUNA, tal como se aprecia en la figura: 5.3, donde lo más verde representa una mayor visibilidad y lo más rojo, la ausencia de visibilidad. También se puede apreciar en la figura 5.4, donde el color verde representa el porcentaje visible y el color rojo lo no visible (el negro representa lo no anunciado, pero no se aprecia pues en este caso se anuncia el 100 % de las redes).

Esto indica que IPv6 se encuentra aún en desarrollo, aún no está implementado en todo el mundo, por lo tanto aún existen dificultades para comunicarse usando este protocolo.

Al repetir el estudio durante varios días de diciembre 2009 y enero 2010, se aprecia que las visibilidades no cambian mucho, la visibilidad para IPv4 se mantiene siempre cercana al 100 %, mientras que para IPv6, se mantiene alrededor de 82 %, manteniéndose las mismas

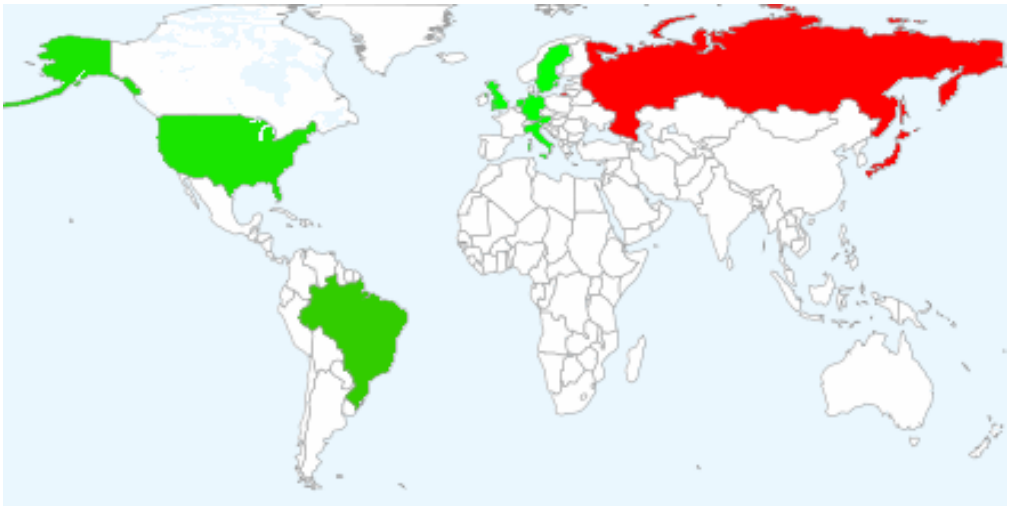

Figura 5.3: Visibilidad de las redes chilenas IPv6 en el mundo el 18-11-2009.

Figura 5.4: Visibilidad de las redes IPv6 de REUNA el mundo el 18-11-2009.

redes sin ser vistas.

Un hecho interesante fue la aparición de la red IPv6 de VTR, en la figura 5.5. La primera aparición fue detectada por el sistema el día 10 de diciembre de 2009, en esta fecha VTR comienza a publicar su red IPv6, y el 17 de ese mes, la red es visible en 11 de los 13 recolectores, es decir en todos los que ven redes IPv6. Esto aumentó la visibilidad promedio de las redes IPv6 chilenas desde 81,54 % hasta 82,05 %.

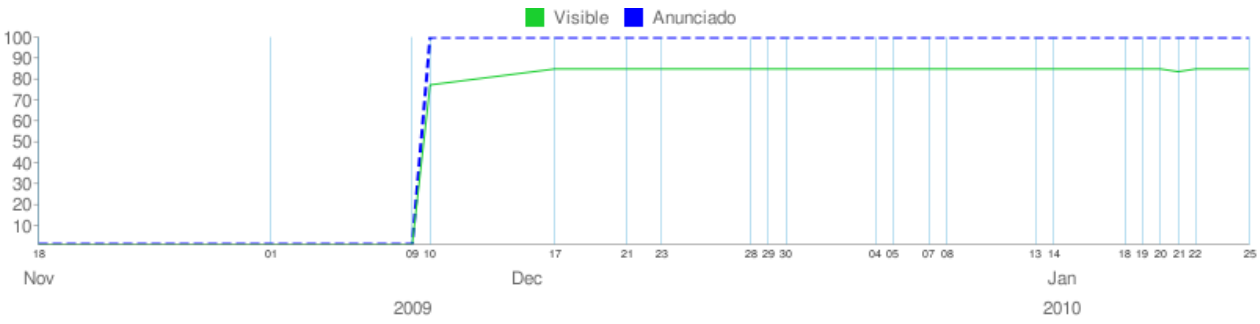

Figura 5.5: Serie Temporal Redes IPv6 Anunciadas y Visibles de la empresa VTR Banda Ancha S.A.

5.3. Evaluación del sistema

Con respecto a el tiempo que demora el sistema en procesar los datos, se tiene que lo que más tiempo consume es el descargar los datos, proceso que demora más de 13 minutos, en cambio el preprocesamiento toma cerca de 3 minutos, al igual que el procesamiento. Esta velocidad de procesamiento es suficiente, pues los datos se descargan y procesan una vez al día. Los gráficos generados permitieron detectar rápidamente los cambios en el tiempo, una vez que se tienen los conocimientos asociados (por ejemplo conocer cuáles son las empresas que cuentan con IPv6).

5.4. Resumen

En este capítulo se analizaron los resultados obtenidos al realizar las mediciones sobre las redes chilenas. En el siguiente capítulo se condensarán las principales conclusiones obtenidas, así como también se plantearán mejoras al sistema, como trabajo futuro.

Capítulo 6

Conclusiones

En el capítulo anterior se revisaron los resultados obtenidos al usar la herramienta desarrollada en esta memoria. En este capítulo se condensan las conclusiones que se pueden obtener a partir del trabajo realizado.

En primer lugar, se definieron los conceptos de redes anunciadas y redes visibles en función de su aparición en tablas de rutas específicas, las de los recolectores, y se ponderó por el tamaño de las redes para obtener valores agregados.

Se seleccionaron recolectores ubicados en distintos países, incluyendo varios países europeos, Rusia, Japón, Estados Unidos y Brasil. Esto permitió tener una mejor visión de la conectividad y menos sesgada que la que se obtendría usando sólo datos de un país o continente.

Se construyó una herramienta capaz de medir la visibilidad de las redes chilenas. Esta herramienta procesa datos diariamente y permite la visualización de estos en cualquier momento y por cualquier persona con acceso a Internet. Los datos pueden ser visualizados en forma agregada, apoyado por gráficos generados dinámicamente, o al detalle. Lo que permite por un lado tener una visión global y por otro revisar los puntos específicos de conflictos.

Las conclusiones obtenidas usando la herramienta son:

1. A la fecha Chile cuenta con 683 redes IPv4, de las cuales menos de un 30 % está en

uso. En IPv6 hay 13 redes, y sólo 6 son usadas. Además se constata que IPv6 aún no está implementada en todo el mundo, pues hay recolectores que no tienen en su tabla de rutas ninguna red IPv6.

2. La herramienta desarrollada, permite además visualizar los cambios ocurridos en el tiempo, como la aparición de nuevas redes o la desaparición de éstas. Esto permite apreciar el crecimiento de IPv6, donde hay aún muy pocas redes y cada nueva red representa un porcentaje significativo del total.

3. A la fecha Chile presenta una alta visibilidad de sus redes estudiado, siendo ésta de 99,99 % para IPv4 y de 82,05 % para IPv6. La sensación es que las redes tienen una configuración adecuada y que esta no es modificada muy frecuentemente.

4. La herramienta es flexible, con otra configuración, podría usarse para medir las visibilidades de otros países para comparar. Además se pueden agregar más recolectores, para obtener una visión aún más amplia. Estos dos puntos quedan propuestos como trabajo futuro.

En general el sistema generado logra su objetivo, realizar una medición de la visibilidad de las redes chilenas y estas resultan ser visibles en el mundo.

6.1. Trabajo futuro

Entre las alternativas que se fueron presentando, hubo algunas que son interesantes de desarrollar, lamentablemente, al tener un tiempo limitado para desarrollar el estudio, no fue posible implementar todas estas ideas. Se presentan ahora las que se consideraron más interesantes para ser trabajadas en el futuro.

Si bien en este trabajo, se cuenta con recolectores en varios continentes, son todos estos recolectores manejados por RIPE, lo que facilitó enormemente su procesamiento, pero por otro lado, puede introducir algún tipo de sesgo. Es por esto que es recomendable agregar más recolectores al sistema. Para hacer esto, hay que ver como descargar y preprocesar los

datos, y agregar los recolectores a la base de datos. Con esto se podría tener una visión más general, que incluya los continentes que no se han incluido y otras entidades recolectoras.

Acerca de la forma de calcular los valores agregados, en este momento se realiza un promedio simple, pero como se mencionó existen otras formas, como ponderar por densidad de internet, o definir alguna otra métrica para medir algún tipo de interacción específica.

Para realizar el estudio para otros países o regiones, basta cambiar la configuración inicial, es decir el seleccionar las redes que se buscarán. Sin embargo para medir más de un país se requieren cambios mayores, en particular definir otros niveles de agregación. En este momento el sistema tiene dos niveles de agregación, a nivel de empresa y a nivel país. Sería ideal poder tener distintos niveles, por ejemplo poder seleccionar todas las universidades, o todos los ISP.

Estos cambios requerirían varias modificaciones a la base de datos y al proceso de visualización, pero como los datos son los mismos, no requeriría mayor cambio en las otras partes del sistema.

Otro punto interesante es el cuándo se calculan los valores agregados. En este momento la mayoría es calculado al momento de desplegarse, esto puede ser razonable si los cálculos son pocos y si se pretende tener varios niveles de agregación distinto. Sin embargo, si se realizan muchos cálculos, se sobrecarga el servidor, en este caso convendría precalcular todos los datos y almacenarlos en la base de datos, de esta forma no se realiza procesamiento adicional al momento de desplegar la información, liberando de carga al servidor. Este cambio requeriría cambiar la base de datos y modificar fuertemente el procesamiento y la visualización de los datos.

Actualmente la frecuencia de recolección de datos es diaria, lo que se consideró apropiado para medir un histórico, pero puede no ser suficiente si sea medir con presición, por ejemplo, la velocidad de recuperación en casos particulares de fallas masivas, como cortes de luz. En estos casos se requiere tener una mayor frecuencia de recolección de datos. Las tablas completas BGP son publicadas por RIPE cada 8 horas, modificar el sistema para descargarlas y procesarlas con esa frecuencia no es muy trabajoso, requiere simplemente cambios en la base de datos y en la frecuencia de descarga, sin embargo aumentar a una mayor presición

sí requiere cambios profundos. RIPE publica las actualizaciones cada 5 minutos, pero estos datos deben ser interpretados para poder extraer información, por lo que se requeriría cambios en el subsistema de procesamiento, además de los ya mencionados.

Referencias

[1] Abilene. http://noc.net.internet2.edu/i2network/research-data.html.

[2] Dan Ardelean. libbgpdump. http://www.ris.ripe.net/source/.

[3] L. Blunk, M. Karir, and C. Labovitz. Mrt routing information export format. http://tools.ietf.org/id/draft-ietf-grow-mrt-04.txt.

[4] Martin Brown. Pakistan hijacks youtube. http://www.renesys.com/blog/2008/02/pakistan-hijacks-youtube-1.shtml.

[5] Kevin Butler, Patrick McDaniel, and William Aiello. Optimizing bgp security by exploiting path stability. In *CCS '06: Proceedings of the 13th ACM conference on Computer and communications security*, pages 298–310, New York, NY, USA, 2006. ACM.

[6] Cakephp. http://cakephp.org.

[7] Lance Cockcroft. Understanding the protocols underlying dynamic routing. http://articles.techrepublic.com.com/5100-10878_11-1052842.html.

[8] S. Deering and R. Hiden. Internet protocol. http://tools.ietf.org/html/2460.

[9] Defcon. http://www.defcon.org.

[10] Xenofontas Dimitropoulos, Dmitri Krioukov, Marina Fomenkov, Bradley Huffaker, Young Hyun, kc claffy, and George Riley. As relationships: inference and validation. *SIGCOMM Comput. Commun. Rev.*, 37(1):29–40, 2007.

[11] N. Feamster, D. Andersen, H. Balakrishnan, and F. Kaashoek. Bgp monitor. http://bgp.lcs.mit.edu/.

[12] Lixin Gao. On inferring autonomous system relationships in the internet. *IEEE/ACM Trans. Netw.*, 9(6):733–745, 2001.

[13] Google chart. `http://code.google.com/apis/chart`.

[14] Bradley Huffaker, Marina Fomenkov, David Moore, Evi Nemeth, and Kimberly Claffy. Measurements of the internet topology in the asia-pacific region. `http://www.caida.org/publications/papers/2000/asia_paper/asia_paper.html`.

[15] Craig Labovitz, G. Robert Malan, and Farnam Jahanian. Internet routing instability. *SIGCOMM Comput. Commun. Rev.*, 27(4):115–126, 1997.

[16] Lacnic delegated resources. `ftp://ftp.lacnic.net/pub/stats/lacnic/delegated-lacnic-latest`.

[17] Bgp4.as, bgp ipv4/ipv6 looking glass servers - bgp route servers. `http://www.bgp4.as/looking-glasses`.

[18] Jun Li, Michael Guidero, Zhen Wu, Eric Purpus, and Toby Ehrenkranz. Bgp routing dynamics revisited. *SIGCOMM Comput. Commun. Rev.*, 37(2):5–16, 2007.

[19] Information Sciences Institute University of Southern California. Internet protocol. `http://tools.ietf.org/html/791`.

[20] Ricardo V. Oliveira, Mohit Lad, and Lixia Zhang. Cyclops. `http://cyclops.cs.ucla.edu`.

[21] Packet clearing house. `http://www.pch.net/home/index.php`.

[22] Alex Pilosov and Anton Kapela. Stealing the internet. In *Defcon 16*, 2008.

[23] Y. Rekhter, T. Li, and S. Hares. A border gateway protocol 4 (bgp-4). `http://tools.ietf.org/html/rfc1771`.

[24] Y. Rekhter, T. Li, and S. Hares. A border gateway protocol 4 (bgp-4). `http://tools.ietf.org/html/rfc4271`.

[25] Ripe-ncc. routing information service project. `http://www.ripencc.org/projects/ris/tools/index.html`.

[26] Soon Tee Teoh, Supranamaya Ranjan, Antonio Nucci, and Chen-Nee Chuah. Bgp eye: a new visualization tool for real-time detection and analysis of bgp anomalies. In *VizSEC '06: Proceedings of the 3rd international workshop on Visualization for computer security*, pages 81–90, New York, NY, USA, 2006. ACM.

[27] Andree Toonk. Bgpmon. `http://bgpmon.net/`.

[28] University of oregon route views archive project. `http://www.routeviews.org`.

Apéndices

A . Conceptos básicos

AS : Autonomous System o Sistema Autónomo, red que está bajo el control de una organización, se identifica por un número (ASN, Autonomous System Number). Se dice que dos Sistemas Autónomos son vecinos, si tienen una conección directa entre ellos. Dos Sistemas Autónomos vecinos, se comunican mediante el protocolo BGP para intercambiar su información de routing.

IP: IP o Internet Protocol, es un protocolo de comunicación. Se le llama dirección IP o simplemente IP a un número que identifica cada máquina en Internet. Hay dos versiones de IP actualmente en uso, IPv4 e IPv6.

IP versión 4: Una IPv4 es un número entre 0 y 2^{32}, generalmente expresado: A.B.C.D, donde cada letra representa un número entre 0 y 255.

IP versión 6 Una IP versión 6 es un número entre 0 y $16^32 - 1 = 2^128 - 1$ usualmente anotado de la forma A:B:C:D:E:F:G:H, donde cada letra es un número entre 0 y 65535 expresados en hexadecimal (de cuatro dígitos).

La principal diferencia entre ambas versiones es el número de equipos que acepta. La cantidad de direcciones IPv4 es mucho menor que la cantidad en IPv6, de hecho en IPv4 ya se están agotando, por lo que se está realizando, lentamente el cambio hacia IPv6.

Red: Una red se refiere a un conjunto de direcciones IP, esta puede ser de dos tipos, ya sea versión 4 o versión 6. Usualmente se usa la notación IP/N, donde IP es una dirección IP que especifica el comienzo de la red y la segunda parte (N, llamado largo de máscara) es un número de 0 a 32 que especifica el tamaño de la red con la fórmula: tamaño= 2^{32-N} para el caso de las redes IPv4 y con la fórmula tamaño= 2^{128-N} para IPv6. Una red IPv4/20 tiene capacidad para 4094 equipos, mientras que una red IPv4/24 tiene capacidad para 254 equipos. La red 200.128.255.0/24, es el conjunto que contiene todas las redes entre 200.128.255.0 y 200.128.255.255.

BGP: Border Gateway Protocol, protocolo de routing entre sistemas autónomos. Funciona mediante anuncios de nuevas rutas y retiros (withdrawals) de éstas. Los atributos relevantes pare este estudio son dos: la red destino, y el AS Path.

AS Path: Uno de los campos de un mensaje BGP, es el camino de Sistemas Autónomos para llegar a la ruta especificada. Es decir una serie de números que representan los Sistemas Autónomos por los que hay que ir pasando para llegar desde el origen hasta el destino.

Tabla BGP: Es la información que guarda un router que le permite comunicarse a cada destino, contiene todas las redes a las que puede llegar (con sus AS Path), si el destino fue aprendido de forma interna (IGP) es decir por otro router dentro del mismo Sistema Autónomo o externo (EGP) de un router perteneciente a otro AS. Además de otras características adicionales usadas para extensiones específicas.