**Mail para:**

mailto: [grampin@fing.edu.uy](mailto:grampin@fing.edu.uy)

cc: [sergion@fing.edu.uy](mailto:sergion@fing.edu.uy)

cc: [siturria@fing.edu.uy](mailto:siturria@fing.edu.uy)

Hola Eduardo,

Luego de analizar las 2 opciones nos inclinamos por estudiar los logs de BGP.

A continuación te enviamos las dudas que nos surgieron de los 4 puntos que habría que realizar:

**1) updates (o "announcements") duplicados; esto puede dar indicio de anomalías en el funcionamiento del sistema autónomo (AS) que produce los duplicados.**

Los updates (o announcements) duplicados se reflejan en líneas exactamente idénticas?

Según ejemplo:

BGP4MP|07/31/13 23:55:08|A|202.249.2.185|25152|177.54.121.0/24|25152 2914 6762 7738 53142|IGP

BGP4MP|07/31/13 23:55:08|A|202.249.2.185|25152|177.54.121.0/24|25152 2914 6762 7738 53142|IGP

El sistema autónomo sería 25152?

Esto sería un duplicado announcements para 25152?

BGP4MP|07/31/13 23:59:54|W|202.249.2.185|25152|120.28.62.0/24

BGP4MP|07/31/13 23:59:54|W|202.249.2.185|25152|120.28.62.0/24

Esto sería un duplicado withdraw para 25152?

**2) existencia de múltiples rutas para un prefijo; esto da idea de la diversidad de conectividad del AS origen del prefijo.**

Las múltiples rutas para un prefijo según ejemplo serían:

BGP4MP|07/31/13 23:55:08|A|202.249.2.185|25152|177.54.121.0/24|25152 2914 6762 7738 53142|IGP

BGP4MP|07/31/13 23:55:08|A|202.249.2.185|25152|177.54.121.0/24|25152 6939 7738 53142|IGP

BGP4MP|07/31/13 23:55:09|A|202.249.2.185|25152|177.54.121.0/24|25152 2914 6762 7738 53142|IGP

Prefijo: 177.54.121.0/24

Ruta1: 25152 2914 6762 7738 53142

Ruta2: 25152 6939 7738 53142

Esto es correcto?

**3) estadísticas de los "AS\_PATH lenght"; esto permite aproximarse a estudiar el diámetro de internet.**

Cita obtenida de http://es.wikipedia.org/wiki/Border\_Gateway\_Protocol:

*"Si se quisiera utilizar el AS-PATH como método de selección de rutas se escogería el que tuviera una lista AS-PATH más pequeña. Esto es una forma de medir que haya menos saltos hacia el destino aunque no es exactamente así porque no se tienen en cuenta los posibles saltos debidos a los routers dentro de un sistema autónomo."*

En base a lo que se menciona en la wiki, el AS\_PATH lenght es la cantidad de los elementos de la lista de AS-PATH?

Según ejemplo:

BGP4MP|07/31/13 23:55:08|A|202.249.2.185|25152|177.54.121.0/24|25152 2914 6762 7738 53142|IGP

BGP4MP|07/31/13 23:55:08|A|202.249.2.185|25152|177.54.121.0/24|25152 6939 7738 53142|IGP

BGP4MP|07/31/13 23:55:09|A|202.249.2.185|25152|177.54.121.0/24|25152 2914 6762 7738 53142|IGP

El prefijo 177.54.121.0/24 tiene 2 length:

Length1 para 25152 2914 6762 7738 53142: 5

Length2 para 25152 6939 7738 53142: 4

Esto es correcto?

**4) "top talkers": que ASes generan más prefijos y/o son más "habladores" por unidad de tiempo. Si además se correlacionan updates y withrawals, se pueden detectar ASes que tienen problemas de configuración del routing interno que se reflejan en el BGP.**

Según ejemplo:

BGP4MP|07/31/13 23:59:24|A|202.249.2.185|25152|222.127.0.0/24|25152 6939 4775|IGP

BGP4MP|07/31/13 23:59:24|W|202.249.2.185|25152|222.127.0.0/24

BGP4MP|07/31/13 23:59:54|A|202.249.2.185|25152|120.28.62.0/24|25152 6939 4775|IGP

El sistema autónomo 25152 generó dos prefijos:

Prefijo1: 222.127.0.0/24

Prefijo2: 120.28.62.0/24

Esto es correcto?

**Si además se correlacionan updates y withrawals, se pueden detectar ASes que tienen problemas de configuración del routing interno que se reflejan en el BGP.**

Esto sería, para el 25152 anterior cuantos son withrawals?

Esperamos tu respuesta para seguir avanzando.

Gracias.